Manuale prodotto GFI

GFI LanGuard™

Guida dell'amministratore

Le informazioni e il contenuto del presente documento vengono forniti esclusivamente a scopi informativi e “come sono”, senza garanzia di alcun tipo, sia espressa che implicita, ivi incluse, in via esemplificativa, tutte le garanzie implicite di commerciabilità, idoneità a soddisfare uno scopo particolare e non violazione dei diritti altrui. GFI Software non sarà ritenuta responsabile di nessun danno, inclusi danni consequenziali, che possano derivare dall’uso del presente documento. Le informazioni sono state ottenute da fonti pubblicamente disponibili. Nonostante siano stati compiuti sforzi ragionevoli al fine di garantire la precisione dei dati forniti, GFI non garantisce, promette né tantomeno assicura la completezza, la precisione, l’aggiornamento o l’adeguatezza di tali dati e non sarà ritenuta responsabile di errori di stampa. GFI non fornisce garanzie, né espresse né implicite e non si assume la responsabilità legale della precisione o della completezza delle informazioni contenute nel presente documento.

Se si ritiene che vi siano errori effettivi nel presente documento, contattarci. Provvederemo a risolvere la cosa quanto prima.

Tutti i nomi di prodotti e società riportati possono essere marchi registrati dei rispettivi proprietari.

GFI LanGuard è un copyright di GFI SOFTWARE Ltd. - 1999-2012 GFI Software Ltd. Tutti i diritti riservati.

Versione documento: 11.1

Ultimo aggiornamento (mese/giorno/anno): 08/04/2013

Sommario

1 Introduzione **16**

1.1 Funzionamento di GFI LanGuard 16
1.2 Funzionamento degli agenti di GFI LanGuard 17
1.3 Funzionamento degli agenti relay di GFI LanGuard 17
1.4 Componenti di GFI LanGuard 18
1.5 Informazioni sulla presente guida 18
1.5.1 Termini e convenzioni utilizzati nel presente manuale 18

2 Installazione di GFI LanGuard **19**

2.1 Scenari di distribuzione 19
2.1.1 Distribuzione di GFI LanGuard in modalità mista 19
2.1.2 Distribuzione di GFI LanGuard con agenti relay 20
2.1.3 Distribuzione di GFI LanGuard in modalità senza agente 21
2.2 Requisiti di sistema 23
2.2.1 Requisiti hardware 23
2.2.2 Requisiti software 24
2.2.3 Porte firewall e protocolli 25
2.2.4 Autorizzazioni gateway 26
2.2.5 Applicazioni antivirus/antispyware supportate 27
2.3 Importazione ed esportazione delle impostazioni 27
2.3.1 Esportazione delle configurazioni in un file 27
2.3.2 Importazione configurazioni da file 28
2.3.3 Importazione delle configurazioni desiderate da un'altra istanza di GFI LanGuard. 29
2.4 Aggiornamento da versioni precedenti 30
2.5 Nuova installazione 32
2.6 Azioni post-installazione 35
2.7 Verifica dell'installazione 37

3 Ottenere risultati **39**

3.1 Valutazione efficace delle vulnerabilità 39
3.2 Gestione efficace delle patch 40
3.3 Utilizzo di GFI LanGuard per la tracciabilità asset 41
3.4 Analisi di rete e software aggiornata 42
3.5 Conformità a PCI DSS 43

4 Gestione degli agenti **44**

4.1 Distribuzione degli agenti 44
4.2 Distribuzione manuale agenti 46
4.3 Proprietà agente 49
4.4 Impostazioni agenti 53
4.5 Configurazione degli agenti relay 54
4.5.1 Configurazione di un agente come relay 55
4.5.2 Configurazione delle opzioni avanzate di un agente relay 59
4.5.3 Connessione di computer a un relay 61
4.6 Gestione dei gruppi agente 62

5 Scansione della rete **65**
5.1 Informazioni sui profili di scansione 65
5.2 Profili di scansione disponibili 65
5.2.1 Scansioni complete/combinate 66
5.2.2 Valutazione delle vulnerabilità 66
5.2.3 Controllo rete e software 67
5.3 Scansioni manuali 67
5.4 Abilitazione dei criteri di controllo di protezione 71
5.5 Scansioni pianificate 72
5.5.1 Creazione di una scansione pianificata 73
5.5.2 Modifica impostazioni scansione pianificata 81
5.5.3 Configurazione proprietà scansione pianificata 81
5.6 Scansioni pianificate agente 82
5.6.1 Avvio di una scansione agente manuale 84

6 Dashboard **85**
6.1 Ottenimento dei risultati dal dashboard 85
6.2 Utilizzo del Dashboard 86
6.3 Utilizzo della struttura computer 86
6.3.1 Filtro semplice 87
6.3.2 Filtro avanzato 87
6.3.3 Raggruppamento 88
6.3.4 Ricerca 89
6.4 Utilizzo attributi 90
6.4.1 Assegnazione attributi a un computer 90
6.4.2 Assegnazione attributi a un gruppo 91
6.4.3 Configurazione attributi 91
6.5 Azioni Dashboard 92
6.6 Esportazione elenco problemi 93
6.7 Visualizzazioni Dashboard 93
6.7.1 Panoramica 94
6.7.2 Visualizzazione Computer 97
6.7.3 Visualizzazione Cronologia 100
6.7.4 Visualizzazione vulnerabilità 101
6.7.5 Visualizzazione Patch 102
6.7.6 Visualizzazione Porte 103
6.7.7 Visualizzazione Software 104
6.7.8 Visualizzazione Hardware 105
6.7.9 Visualizzazione Informazioni di sistema 106

7 Interpretazione risultati **107**
7.1 Interpretazione risultati scansione manuale 107
7.1.1 Visualizzazione risultati di scansione 107
7.1.2 Valutazione del livello di vulnerabilità 109
7.1.3 Valutazione delle vulnerabilità 111
7.1.4 Controllo rete e software 112
7.2 Caricamento dei risultati dal database 117

7.3 Salvataggio e caricamento dei risultati XML 118

8 Riparazione vulnerabilità **120**

8.1 Riparazione automatica 120
8.1.1 Note sulla riparazione automatica 120
8.1.2 Configurazione della distribuzione automatica degli aggiornamenti mancanti 121
8.1.3 Configurazione della disinstallazione automatica delle applicazioni non autorizzate 126
8.1.4 Configurazione delle opzioni di riparazione automatica 130
8.1.5 Configurazione delle opzioni di riavvio e arresto utente finale 137
8.1.6 Configurazione dei messaggi della riparazione automatica 137
8.1.7 Configurazione della riparazione automatica agenti 141
8.2 Riparazione manuale 143
8.2.1 Note sulla riparazione manuale 143
8.2.2 Utilizzo del Centro riparazioni 143
8.2.3 Distribuzione aggiornamenti software 144
8.2.4 Disinstallazione aggiornamenti software 147
8.2.5 Distribuzione software personalizzato 149
8.2.6 Disinstallazione delle applicazioni personalizzate 151
8.2.7 Protezione antimalware 152
8.2.8 Utilizzo del supporto del desktop remoto 154

9 Attività di monitoraggio **156**

9.1 Monitoraggio scansioni di sicurezza 156
9.1.1 Filtra scansioni di sicurezza 157
9.2 Monitoraggio download aggiornamenti software 158
9.2.1 Risoluzione problemi aggiornamenti software non riusciti 159
9.3 Monitoraggio operazioni di riparazione 160
9.3.1 Sottoscheda Operazioni di riparazione 160
9.3.2 Visualizzazione Operazioni di riparazione 162
9.4 Monitoraggio aggiornamenti prodotto 163

10 Creazione di rapporti **164**

10.1 Rapporti disponibili 164
10.1.1 Rapporti generali 164
10.1.2 Rapporti di conformità legale 167
10.2 Generazione report 171
10.3 Pianificazione dei rapporti 173
10.3.1 Creazione di nuovi rapporti pianificati 173
10.3.2 Configurazione opzioni rapporti pianificati 175
10.3.3 Gestione rapporti pianificati 175
10.4 Personalizzazione rapporti predefiniti 176
10.4.1 Creazione rapporti personalizzati 176
10.4.2 Personalizzazioni loghi rapporto 178
10.4.3 Personalizzazione formato rapporto e-mail 179
10.5 Ricerca nel testo completo 180

11 Personalizzazione di GFI LanGuard **183**

11.1 Configurazione delle opzioni di avviso 183
11.2 Configurazione opzioni di manutenzione database 184
11.2.1 Utilizzo di Access™ come database back-end 184
11.2.2 Utilizzo di SQL Server® come database back-end 185
11.2.3 Gestione dei risultati della scansione salvati 187
11.2.4 Elenco dei computer sottoposti a scansione 188
11.2.5 Configurazione opzioni di manutenzione database avanzate 188
11.2.6 Configurazione delle opzioni di conservazione database 189
11.3 Configurazione aggiornamenti del programma 190
11.3.1 Configurazione impostazioni proxy 190
11.3.2 Configurazione opzioni di aggiornamento automatico 191
11.3.3 Installazione manuale degli aggiornamenti del programma 192

12 Editor dei profili di scansione 194

12.1 Creazione di un nuovo profilo di scansione 194
12.2 Configurazione delle vulnerabilità 195
12.2.1 Abilitazione della scansione di vulnerabilità 195
12.2.2 Personalizzazione dell'elenco delle vulnerabilità da sottoporre a scansione 196
12.2.3 Personalizzazione proprietà controlli di vulnerabilità 197
12.2.4 Configurazione delle condizioni dei controlli di vulnerabilità 198
12.3 Configurazione delle patch 205
12.3.1 Abilitazione/Disabilitazione dei controlli di rilevamento delle patch mancanti 206
12.3.2 Personalizzazione dell'elenco delle patch software da sottoporre a scansione 207
12.3.3 Ricerca di informazioni in un bollettino 207
12.4 Configurazione opzioni di controllo rete e software 208
12.4.1 Configurazione opzioni di scansione per la porta TCP/UDP 209
12.4.2 Configurazione opzioni Informazioni di sistema 210
12.4.3 Configurazione opzioni di scansione dei dispositivi 210
12.4.4 Configurazione delle opzioni di scansione delle applicazioni 213
12.5 Configurazione delle opzioni di scansione di sicurezza 217

13 Programmi di utilità 220

13.1 Ricerca DNS 220
13.2 Traceroute 223
13.3 Whois 224
13.4 Enumera computer 225
13.4.1 Avvio di una scansione di sicurezza 226
13.4.2 Distribuzione di patch personalizzate 226
13.4.3 Abilitazione dei criteri di controllo 226
13.5 Enumera utenti 227
13.6 Controllo SNMP 228
13.7 Esplorazione SNMP 229
13.8 Controllo SQL Server® 230
13.9 Strumenti riga di comando 231
13.9.1 Utilizzo di Insscmd.exe 231
13.9.2 Utilizzo di deploycmd.exe 232
13.9.3 Utilizzo di impex.exe 234

14 Script Debugger **237**
14.1 Creazione di script personalizzati tramite VBscript 237
14.1.1 Aggiunta di un controllo di vulnerabilità che utilizza uno script VBScript (.vbs) personalizzato 237
14.2 Creazione di script personalizzati utilizzando il linguaggio di scripting Python 242
14.3 Modulo SSH 246
14.3.1 Parole chiave 246
14.3.2 Aggiunta di un controllo delle vulnerabilità che utilizza uno script di shell personalizzato 247

15 Funzioni varie **252**
15.1 Configurazione di NetBIOS 252
15.2 Disinstallazione GFI LanGuard 253

16 Risoluzione dei problemi e supporto **254**
16.1 Risoluzione di problemi comuni 254
16.2 Utilizzo della risoluzione guidata dei problemi 256
16.3 GFI SkyNet 258
16.4 Forum Web 258
16.5 Richiesta di supporto tecnico 258

17 Appendice 1 - Dati elaborati **260**
17.1 Stato dell'applicazione di patch al sistema 260
17.2 Porte 261
17.3 Hardware 261
17.4 Software 263
17.5 Informazioni di sistema 266

18 Appendice 2 - Certificazioni **268**
18.1 Open Vulnerability and Assessment Language (OVAL) 268
18.1.1 Supporto OVAL in GFI LanGuard 268
18.1.2 Informazioni sulla compatibilità OVAL 269
18.1.3 Invio di rapporti degli errori OVAL 269
18.2 Common Vulnerabilities and Exposures (CVE) 269
18.2.1 Informazioni sulla compatibilità CVE 269
18.2.2 Informazioni su CVE e CAN 270
18.2.3 Ricerca di voci CVE 270
18.2.4 Recupero dei nomi CVE 271
18.2.5 Importazione ed esportazione dei dati CVE 271

19 Glossario **272**

20 Indice **280**

Elenco figure

Screenshot 1: Esportazione configurazioni in un file 28
Screenshot 2: Importazione configurazioni da file 29
Screenshot 3: Importazione impostazione 30
Screenshot 4: Finestra di dialogo Controllo prerequisiti 31
Screenshot 5: Importazione ed esportazione delle impostazioni di un'istanza precedente 32
Screenshot 6: Contratto di licenza con l'utente finale 33
Screenshot 7: Specifica dei dati dell'utente e della chiave di licenza 33
Screenshot 8: Credenziali servizio attendant 34
Screenshot 9: Importazione ed esportazione configurazioni 36
Screenshot 10: Avvia una scansione 37
Screenshot 11: Proprietà di Avvia una scansione 37
Screenshot 12: Riepilogo risultati di scansione 38
Screenshot 13: Gestisci agenti 45
Screenshot 14: Aggiungi altri computer - Selezione del tipo per l'importazione 47
Screenshot 15: Aggiungi altri computer - Assegnazione di attributi ai nuovi computer 48
Screenshot 16: Proprietà agente - scheda Generale 49
Screenshot 17: Proprietà agente - scheda Stato agente 50
Screenshot 18: Proprietà agente - scheda Attributi 51
Screenshot 19: Proprietà agente - scheda Relay 52
Screenshot 20: Impostazioni agente - scheda Generale 53
Screenshot 21: Impostazioni agente - scheda Avanzate 54
Screenshot 22: Finestra di dialogo Proprietà agente 56
Screenshot 23: Imposta computer come procedura guidata relay 57
Screenshot 24: Scegliere la directory di memorizzazione nella cache per il nuovo agente relay 58
Screenshot 25: Passaggio riepilogativo delle impostazioni 59
Screenshot 26: Proprietà agente relay - Impostazioni avanzate 60
Screenshot 27: Finestra di dialogo delle impostazioni avanzate dell'agente relay 60
Screenshot 28: Connessione a un agente relay 62
Screenshot 29: Attributi agente 63
Screenshot 30: Relay agente 64
Screenshot 31: Impostazioni Scansione manuale 68
Screenshot 32: Proprietà personalizzate destinazione 69
Screenshot 33: Aggiungi nuova regola... 70
Screenshot 34: Procedura guidata Amministrazione criteri di controllo 72
Screenshot 35: Finestra di dialogo Nuova scansione pianificata 73
Screenshot 36: Frequenza scansione pianificata 74
Screenshot 37: Scelta profilo di scansione 75
Screenshot 38: Credenziali di accesso remoto 76

Screenshot 39: Opzioni di creazione dei rapporti della scansione pianificata 77
Screenshot 40: Opzioni di riparazione automatica della scansione pianificata 78
Screenshot 41: Opzioni di creazione dei rapporti della scansione pianificata 79
Screenshot 42: Opzioni di creazione dei rapporti della scansione pianificata 80
Screenshot 43: Proprietà scansione pianificata 82
Screenshot 44: Ricorrenza attività agente 83
Screenshot 45: Visualizza dashboard 86
Screenshot 46: Filtro semplice 87
Screenshot 47: Aggiungi proprietà filtro 88
Screenshot 48: Ricerca di computer e gruppi specifici 89
Screenshot 49: Assegnazione attributi: Computer singolo 90
Screenshot 50: Assegnazione attributi: Più computer 91
Screenshot 51: Finestra di dialogo Nuovo attributo 92
Screenshot 52: Sezione Azioni del Dashboard 92
Screenshot 53: Panoramica Dashboard 94
Screenshot 54: Analisi risultati per computer 97
Screenshot 55: Visualizzazione Cronologia nel Dashboard 100
Screenshot 56: Visualizzazione Vulnerabilità nel Dashboard 101
Screenshot 57: Visualizzazione Patch nel Dashboard 102
Screenshot 58: Visualizzazione Porte nel Dashboard 103
Screenshot 59: Visualizzazione Software nel Dashboard 104
Screenshot 60: Visualizzazione Hardware nel Dashboard 105
Screenshot 61: Visualizzazione Informazioni di sistema nel Dashboard 106
Screenshot 62: Panoramica risultati 108
Screenshot 63: Misurazione del livello di vulnerabilità 109
Screenshot 64: Misurazione del livello di vulnerabilità del dashboard 110
Screenshot 65: Nodo di valutazione delle vulnerabilità 111
Screenshot 66: Finestra di dialogo Info bollettino 112
Screenshot 67: Nodo Controllo rete e software 113
Screenshot 68: Stato patch di sistema 114
Screenshot 69: Tutte le porte UDP e TCP rilevate durante una scansione 114
Screenshot 70: Risultati della scansione ricaricati 118
Screenshot 71: Distribuzione automatica delle patch 122
Screenshot 72: Opzioni avanzate di distribuzione automatica delle patch 123
Screenshot 73: Configurazione proprietà di download automatico patch 125
Screenshot 74: Impostazioni di archivio patch 126
Screenshot 75: Applicazione non autorizzata 127
Screenshot 76: Procedura guidata Inventario applicazioni 128
Screenshot 77: Convalida della disinstallazione automatica delle applicazioni 129
Screenshot 78: Proprietà computer 130

Screenshot 79: Impostazioni generali di riparazione automatica 131
Screenshot 80: Opzioni preliminari alla distribuzione 132
Screenshot 81: Opzioni successive alla distribuzione 133
Screenshot 82: Opzioni di distribuzione avanzate 134
Screenshot 83: Gestione dispositivi 135
Screenshot 84: Risparmio energia 136
Screenshot 85: Opzioni di riavvio/arresto 137
Screenshot 86: Centro riparazioni - Distribuisci aggiornamenti software 138
Screenshot 87: Finestra di dialogo Opzioni di distribuzione 139
Screenshot 88: Opzioni prima della distribuzione 140
Screenshot 89: Personalizzazione messaggi di avviso 141
Screenshot 90: Riparazione automatica agente 142
Screenshot 91: Centro riparazioni 144
Screenshot 92: Distribuzione aggiornamenti software 145
Screenshot 93: Opzioni di Distribuisci aggiornamenti software 146
Screenshot 94: Disinstallazione aggiornamenti software 147
Screenshot 95: Opzioni di Disinstalla aggiornamenti software 148
Screenshot 96: Elenco di software da distribuire 150
Screenshot 97: Disinstallazione applicazioni 151
Screenshot 98: Protezione antimalware 153
Screenshot 99: Connessione desktop remoto 154
Screenshot 100: Monitoraggio scansioni di sicurezza 156
Screenshot 101: Finestra di dialogo Filtra scansioni di sicurezza 157
Screenshot 102: Download aggiornamenti di sicurezza 158
Screenshot 103: Monitoraggio delle operazioni dalla sottoscheda Operazioni di riparazione 161
Screenshot 104: Monitoraggio delle operazioni dalla visualizzazione Operazioni di riparazione 162
Screenshot 105: Attività aggiornamenti prodotto 163
Screenshot 106: Rapporto di esempio - Parte 1 171
Screenshot 107: Rapporto di esempio - Parte 2 172
Screenshot 108: Rapporto di esempio - Parte 3 172
Screenshot 109: Selezionare il modello del rapporto pianificato 173
Screenshot 110: Aggiunta o rimozione di domini di destinazione e/o computer 173
Screenshot 111: Modifica opzioni rapporti pianificati 176
Screenshot 112: Monitoraggio attività rapporti pianificati 176
Screenshot 113: Modifica impostazioni rapporto dall'anteprima di esempio del rapporto 177
Screenshot 114: Configurazione elementi rapporto 177
Screenshot 115: Configurazione opzioni filtro rapporto 178
Screenshot 116: Configurazione opzioni di raggruppamento e ordinamento del rapporto 178
Screenshot 117: Personalizzazione dei parametri del rapporto 181
Screenshot 118: Navigazione mediante i collegamenti dei rapporti 182

Screenshot 119: Configurazione delle opzioni di avviso 183
Screenshot 120: Finestra di dialogo Proprietà di manutenzione del database 185
Screenshot 121: Opzioni database back-end SQL Server® 186
Screenshot 122: Proprietà manutenzione del database: scheda Gestisci risultati della scansione salvati 187
Screenshot 123: Proprietà manutenzione del database: scheda Avanzate 189
Screenshot 124: Configurazione delle impostazioni del server proxy 191
Screenshot 125: Configurazione aggiornamenti all'avvio dell'applicazione 192
Screenshot 126: Procedura guidata Verifica disponibilità aggiornamenti 193
Screenshot 127: Editor del profilo di scansione 195
Screenshot 128: Abilitazione della scansione di vulnerabilità per il profilo di scansione selezionato 196
Screenshot 129: Selezionare i controlli di vulnerabilità eseguiti da questo profilo di scansione 197
Screenshot 130: Finestra di dialogo Proprietà vulnerabilità: scheda Generale 198
Screenshot 131: Scheda di configurazione delle condizioni di vulnerabilità 199
Screenshot 132: Procedura guidata Proprietà controllo - Selezione del tipo di controllo 200
Screenshot 133: Procedura guidata Proprietà controllo - Definizione dell'oggetto da esaminare 201
Screenshot 134: Procedura guidata Proprietà controllo - Impostazione delle condizioni necessarie 202
Screenshot 135: Procedura guidata Proprietà controllo - Definizione degli operatori condizionali 203
Screenshot 136: Opzioni avanzate di vulnerabilità 204
Screenshot 137: Finestre di dialogo Scansione delle vulnerabilità avanzate 205
Screenshot 138: Proprietà Profili di scansione: opzioni scheda Patch 206
Screenshot 139: Selezionare le patch mancanti da enumerare 207
Screenshot 140: Ricerca di informazioni in un bollettino 207
Screenshot 141: Informazioni estese del bollettino 208
Screenshot 142: Proprietà Profili di scansione: opzioni scheda Porte TCP 209
Screenshot 143: Proprietà Profili di scansione: opzioni della scheda Informazioni di sistema 210
Screenshot 144: Pagina di configurazione dei dispositivi di rete 211
Screenshot 145: Pagina di configurazione delle applicazioni 214
Screenshot 146: Proprietà Profili di scansione: scheda Opzioni di scansione 218
Screenshot 147: Strumento Ricerca DNS 221
Screenshot 148: Opzioni Strumento Ricerca DNS 222
Screenshot 149: Strumento Traceroute 223
Screenshot 150: Strumento Whois 224
Screenshot 151: Strumento Enumera computer 225
Screenshot 152: Finestra di dialogo dello strumento Enumera utenti 227
Screenshot 153: Strumento Controllo SNMP 228
Screenshot 154: Strumento esplorazione SNMP 229
Screenshot 155: Controllo SQL Server® 230
Screenshot 156: Finestra di dialogo Aggiungi vulnerabilità 239
Screenshot 157: Aggiunta di controlli di vulnerabilità - Selezione del tipo di controllo 240
Screenshot 158: Aggiunta di controlli di vulnerabilità - Selezione del file di script VB 241

Screenshot 159: Aggiunta di controlli di vulnerabilità - Definizione delle condizioni 242
Screenshot 160: Finestra di dialogo Aggiungi vulnerabilità 243
Screenshot 161: Aggiunta di controlli di vulnerabilità - Selezione del tipo di controllo 244
Screenshot 162: Aggiunta di controlli di vulnerabilità - Selezione del file di script python 245
Screenshot 163: Aggiunta di controlli di vulnerabilità - Definizione delle condizioni 246
Screenshot 164: Finestra di dialogo Aggiungi vulnerabilità 248
Screenshot 165: Aggiunta di controlli di vulnerabilità - Selezione del tipo di controllo 249
Screenshot 166: Aggiunta di controlli di vulnerabilità - Selezione del file SSH 250
Screenshot 167: Aggiunta di controlli di vulnerabilità - Definizione delle condizioni 251
Screenshot 168: Finestra di dialogo delle proprietà della connessione alla rete locale: scheda WINS 253
Screenshot 169: Risoluzione guidata dei problemi - Dettagli sulle informazioni 257
Screenshot 170: Risoluzione guidata dei problemi - Raccolta delle informazioni sui problemi noti 258
Screenshot 171: Ricerca di informazioni CVE 270

Elenco tabelle

Table 1: Componenti di GFI LanGuard 18
Table 2: Termini e convenzioni utilizzati nel presente manuale 18
Table 3: Requisiti hardware - GFI LanGuard Server 23
Table 4: Requisiti hardware - GFI LanGuard Agente 23
Table 5: Requisiti hardware - GFI LanGuard Agente relay 24
Table 6: Sistemi operativi supportati 24
Table 7: Database back-end supportati 25
Table 8: Requisiti software - Componenti aggiuntivi 25
Table 9: Porte e protocolli 26
Table 10: Opzioni di sostituzione 30
Table 11: Opzioni di sostituzione di importazione 36
Table 12: Selezione destinazione 45
Table 13: Opzioni regole personalizzate 45
Table 14: Distribuisci agenti: Impostazioni avanzate 46
Table 15: Procedura guidata Aggiungi altri computer 47
Table 16: Impostazioni attributi 48
Table 17: Opzioni relay agente 52
Table 18: Impostazioni avanzate agente relay 53
Table 19: Impostazioni agenti 53
Table 20: Agente relay - Opzioni avanzate 61
Table 21: Stato gruppo agente 62
Table 22: Individuazione di rete gruppo agente 63
Table 23: Opzioni relay agente 64
Table 24: Profili di scansioni complete/combinate 66
Table 25: Profili di scansione per la valutazione delle vulnerabilità 66
Table 26: Controllo rete e software 67
Table 27: Opzioni computer di destinazione durante il controllo 68
Table 28: Proprietà personalizzate destinazione 70
Table 29: Opzioni di accesso e di controllo 71
Table 30: Opzioni di scansione 71
Table 31: Nuovo tipo di scansione pianificata 74
Table 32: Credenziali di accesso remoto 76
Table 33: Opzioni di risparmio energetico 77
Table 34: Opzioni di riparazione automatica 78
Table 35: Opzioni di creazione dei rapporti 79
Table 36: Opzioni per la gestione dei profili di scansione 81
Table 37: Proprietà scansione pianificata 82
Table 38: Opzioni di ricerca 89

Table 39: Azioni Dashboard 92
Table 40: Informazioni software dal controllo 94
Table 41: Visualizzazione in base alle informazioni dei computer 97
Table 42: Icone tempo di risposta 108
Table 43: Punteggi di ponderazione del livello di vulnerabilità 109
Table 44: Gruppi di vulnerabilità 111
Table 45: Informazioni hardware dal controllo 115
Table 46: Informazioni software dal controllo 115
Table 47: Informazioni di sistema da un controllo 116
Table 48: Fasi di riparazione automatica 121
Table 49: Opzioni avanzate di distribuzione automatica delle patch 123
Table 50: Gestione scansioni pianificate applicabili 130
Table 51: Prima della distribuzione 132
Table 52: Dopo la distribuzione 133
Table 53: Opzioni di distribuzione avanzate 134
Table 54: Opzioni di distribuzione avanzate 137
Table 55: Messaggi di avviso 141
Table 56: Azioni di riparazione 144
Table 57: Opzioni di Distribuisci aggiornamenti software 146
Table 58: Opzioni di Disinstalla aggiornamenti software 148
Table 59: Opzioni disponibili in Distribuisci software personalizzato 150
Table 60: Opzioni di distribuzione 150
Table 61: Disinstallazione applicazioni 152
Table 62: Opzioni di distribuzione 153
Table 63: Finestra di dialogo Filtra scansioni di sicurezza 158
Table 64: Stato download aggiornamenti 159
Table 65: Download aggiornamenti di sicurezza 159
Table 66: Risoluzione problemi aggiornamenti software non riusciti 160
Table 67: Rapporti generali disponibili 165
Table 68: Rapporti di conformità legale disponibili 168
Table 69: Opzioni modello del rapporto pianificato 173
Table 70: Opzioni Domini e computer di destinazione 174
Table 71: Opzioni di pianificazione 174
Table 72: Impostazioni di avviso e di salvataggio 175
Table 73: Segnaposto rapporto 179
Table 74: Parametri impostazioni di posta 184
Table 75: Opzioni di notifica 184
Table 76: Opzioni di conservazione database 190
Table 77: Impostazioni proxy 191
Table 78: Finestra di dialogo Proprietà vulnerabilità 198

Table 79: Opzioni di scansione della porta TCP 209
Table 80: Opzioni di scansione del dispositivo 212
Table 81: Opzioni di scansione delle applicazioni 214
Table 82: Opzioni scanner 218
Table 83: Opzioni di ricerca DNS 221
Table 84: Icone Traceroute 223
Table 85: Opzioni di Enumera computer 225
Table 86: Parametri di comando insscmd 231
Table 87: Variabili supportate in Inssmcd 232
Table 88: Parametri di comando deploycmd 233
Table 89: Switch di comando impex 234
Table 90: Parole chiave di vulnerabilità 247
Table 91: GFI LanGuard Problemi comuni 254
Table 92: Opzioni di raccolta informazioni 257
Table 93: Compatibilità CVE 269

1 Introduzione

GFI LanGuard che consente una facile gestione della protezione endpoint dei dispositivi presenti nella LAN. Funge da consulente di sicurezza virtuale e offre gestione patch, valutazione delle vulnerabilità e supporto del controllo di rete per i computer basati su Windows®e MAC. GFI LanGuard fornisce la protezione LAN attraverso:

- Identificazione delle debolezze del sistema e della rete tramite un database completo di controlli delle vulnerabilità. Ciò comprende test basati su OVAL, CVE e sulle linee guida di valutazione delle vulnerabilità della Top 20 del SANS
- Controllo di tutte le risorse hardware e software della rete in uso, con la possibilità di creare un inventario dettagliato delle risorse. Il sistema è in grado di enumerare le applicazioni installate e le periferiche connesse alla rete.
- Download automatico e installazione remota dei service pack e delle patch per i sistemi operativi Microsoft® Windows e MAC, oltre che per i prodotti di terze parti.
- Disinstallazione automatica del software non autorizzato.

Argomenti del presente capitolo:

1.1 Funzionamento di GFI LanGuard 16
1.2 Funzionamento degli agenti di GFI LanGuard 17
1.3 Funzionamento degli agenti relay di GFI LanGuard 17
1.4 Componenti di GFI LanGuard 18
1.5 Informazioni sulla presente guida 18

1.1 Funzionamento di GFI LanGuard

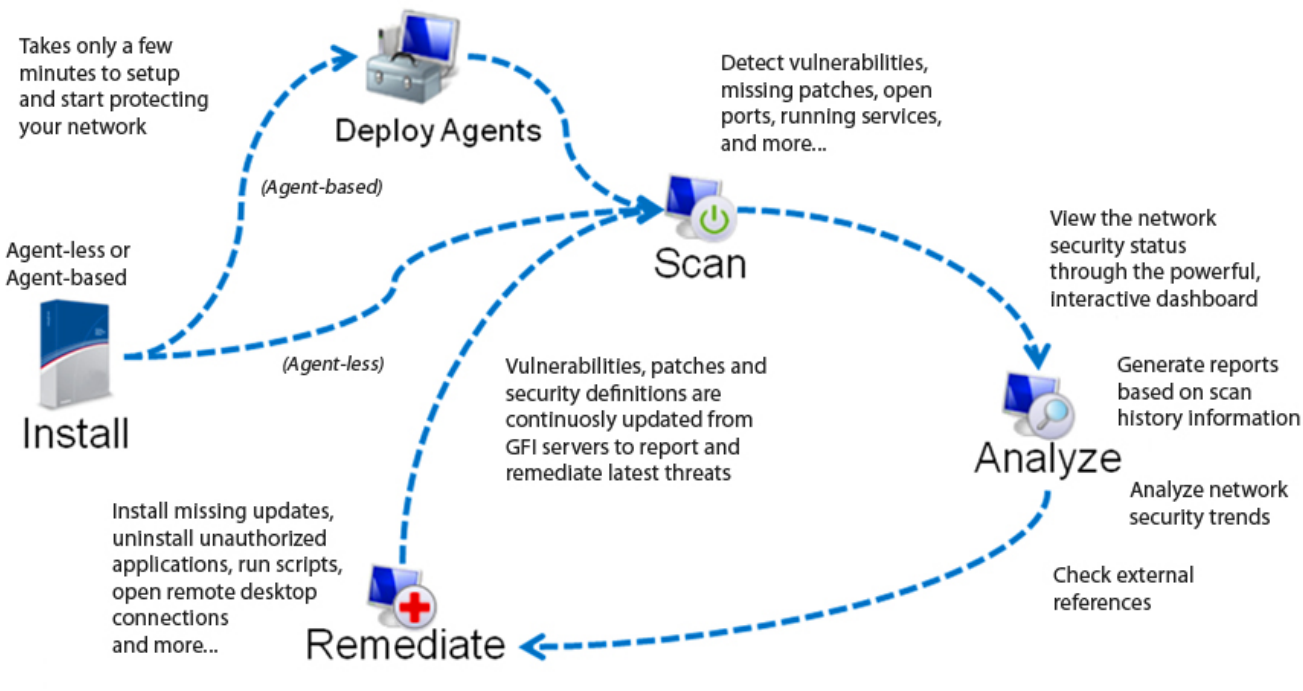

Takes only a few minutes to setup and start protecting your network
Deploy Agents
(Agent-based)
Detect vulnerabilities, missing patches, open ports, running services, and more...
Agent-less or Agent-based
Scan
View the network security status through the powerful, interactive dashboard
(Agent-less)
Vulnerabilities, patches and security definitions are continuosly updated from GFI servers to report and remediate latest threats
Generate reports based on scan history information
Install
Analyze
Analyze network security trends
Install missing updates, uninstall unauthorized applications, run scripts, open remote desktop connections and more...
Check external references
Remediate

Figure 1: Funzionamento di GFI LanGuard

Quando viene installato, GFI LanGuard esegue due operazioni:

- prima di tutto determina i computer raggiungibili. Inoltre tenta di raccogliere le serie di informazioni dai computer di destinazione nell'ambito delle proprie operazioni di individuazione di rete, utilizzando un sottoinsieme di protocolli SMB, NETBIOS e ICMP. Nelle destinazioni supportate sono inclusi l'host locale, l'IP, il nome computer, l'elenco di computer, l'intervallo IP, l'intero dominio/gruppo di lavoro e/o l'unità organizzativa.
- In secondo luogo, una volta identificate le destinazioni, GFI LanGuard effettua una scansione approfondita per enumerare tutte le informazioni relative al computer di destinazione. GFI LanGuard Utilizza una varietà di tecniche per ottenere accesso a queste informazioni, a partire dai controlli di proprietà di file e cartelle, i controlli del registro, i comandi WMI, i comandi SMB oltre ai controlli di scansioni delle porte (TCP/UDP) e altro ancora.

1.2 Funzionamento degli agenti di GFI LanGuard

GFI LanGuard può essere configurato per la rilevazione e la distribuzione automatica degli agenti nei nuovi computer. Gli agenti riducono al minimo l'utilizzo della larghezza di banda della rete. Questo avviene perché, nella modalità senza agente, il componente server GFI LanGuard esegue controlli in rete; mentre con la modalità agente i controlli vengono eseguiti utilizzando le risorse delle destinazioni della scansione e solo un file XML dei risultati viene trasferito nella rete.

Gli agenti inviano i dati di scansione a GFI LanGuard tramite la porta TCP 1070. La porta viene aperta per impostazione predefinita al momento dell'installazione di GFI LanGuard. Gli agenti non impiegano le risorse del computer di destinazione della scansione a meno che questo non esegua una scansione oppure operazioni di riparazione. Se un agente non risponde per 60 giorni, viene automaticamente disinstallato dal computer di destinazione.

Nota

Per impostazione predefinita, gli agenti vengono disinstallati automaticamente dopo 60 giorni. Per personalizzare l'intervallo di tempo, accedere alla scheda **Configurazione> Gestione agenti** e dal riquadro di destra fare clic su **Impostazioni agenti**. Specificare il numero di giorni nella scheda **Generale** della finestra di dialogo **Impostazioni agenti**.

Nota

Gli agenti possono essere solo installati su computer che eseguono sistemi operativi Microsoft Windows e richiedono all'incirca 25 MB di memoria e 350 MB di spazio libero su disco.

1.3 Funzionamento degli agenti relay di GFI LanGuard

GFI LanGuard consente di configurare qualsiasi computer in cui è installato un agente GFI LanGuard affinché funga da server GFI LanGuard. Tali agenti sono denominati **agenti relay**. Gli agenti relay riducono il carico del server GFI LanGuard. I computer configurati come agenti relay scaricano le patch e le definizioni direttamente dal server GFI LanGuard e le inoltrano ai computer client come se fossero il componente server.

1.4 Componenti di GFI LanGuard

La presente sezione fornisce le informazioni relative ai componenti installati per impostazione predefinita al momento in cui si installa GFI LanGuard. Una volta installato il prodotto, è possibile gestire la gestione delle patch e le attività di riparazione dalla Console di gestione. La Console di gestione è considerata anche la componente server di GFI LanGuard, come descritto nella tabella seguente:

Table 1: Componenti di GFI LanGuard

Componente	Descrizione
Server GFI LanGuard	Nota anche come Console di gestione. Consente di gestire gli agenti, eseguire le scansioni, analizzare i risultati, riparare i problemi di vulnerabilità e generare rapporti.
Agenti di GFI LanGuard	Gli agenti consentono di eseguire l'elaborazione e il controllo dei dati nei computer di destinazione: una volta completato il controllo, il risultato viene inviato a GFI LanGuard.
Aggiornamento del sistema GFI LanGuard	Consente di configurare GFI LanGuard affinché scarichi automaticamente gli aggiornamenti rilasciati da GFI al fine di migliorare la funzionalità del programma. Tali aggiornamenti comprendono anche il controllo del sito Web di GFI per verificare la presenza di build più recenti.
GFI LanGuard Attendant Service	Il servizio di background che gestisce tutte le operazioni pianificate comprese le scansioni di sicurezza pianificate sulla rete, la distribuzione di patch e le operazioni di riparazione.
Editor dei profili di scansione GFI LanGuard	L'editor consente di creare profili di scansione nuovi e di modificare quelli esistenti.
Strumenti riga di comando GFI LanGuard	Consentono di lanciare scansioni sulle vulnerabilità della rete e sessioni di distribuzione delle patch, nonché di importare ed esportare profili e vulnerabilità senza caricare la console di gestione GFI LanGuard.

1.5 Informazioni sulla presente guida

Lo scopo della presente Guida dell'amministratore è aiutare gli amministratori di sistema a installare, configurare ed eseguire GFI LanGuard con il minimo sforzo.

1.5.1 Termini e convenzioni utilizzati nel presente manuale

Table 2: Termini e convenzioni utilizzati nel presente manuale

Termine	Descrizione
	Ulteriori informazioni e i riferimenti essenziali per il funzionamento di GFI LanGuard.
	Notifiche e avvertenze importanti riguardo i potenziali problemi rilevati di frequente.
>	Istruzioni di navigazione dettagliate per accedere a una funzione specifica.
Testo in grassetto	Elementi da selezionare quali nodi, opzioni di menu o pulsanti dei comandi.
Testo in corsivo	Parametri e valori da sostituire con valori applicabili, quali percorsi personalizzati e nomi file.
`Codice`	Indica i valori di testo da immettere, come comandi e indirizzi.

2 Installazione di GFI LanGuard

Il presente capitolo guida l'utente nella scelta della soluzione più appropriata che risponde ai propri requisiti oltre a fornire le informazioni relative a una distribuzione corretta di un'istanza pienamente funzionale di GFI LanGuard.

Argomenti del presente capitolo:

2.1 Scenari di distribuzione 19
2.2 Requisiti di sistema 23
2.3 Importazione ed esportazione delle impostazioni 27
2.4 Aggiornamento da versioni precedenti 30
2.5 Nuova installazione 32
2.6 Azioni post-installazione 35
2.7 Verifica dell'installazione 37

2.1 Scenari di distribuzione

GFI LanGuard può essere installato su qualsiasi computer che soddisfi i requisiti minimi di sistema. Utilizzare le informazioni contenute in questa sezione per determinare se si desidera monitorare un pool senza agente o basato su agente oppure una combinazione dei due, a seconda di quanto segue:

- Numero di computer e dispositivi che si desidera monitorare
- Carico del traffico in rete durante i periodi di funzionamento normale.

Nelle sezioni seguenti vengono fornite le informazioni sui diversi scenari di distribuzione supportati da GFI LanGuard:

- Distribuzione di GFI LanGuard in modalità mista
- Distribuzione di GFI LanGuard con agenti relay
- Distribuzione di GFI LanGuard in modalità senza agente

2.1.1 Distribuzione di GFI LanGuard in modalità mista

GFI LanGuard può essere configurato per la distribuzione automatica di agenti sui computer appena rilevati o su quelli selezionati manualmente. Gli agenti consentono di eseguire l'elaborazione e il controllo dei dati nei computer di destinazione: una volta completato il controllo, il risultato viene inviato a GFI LanGuard mediante un file XML. Scansioni basate sull'agente:

- Migliori prestazioni, poiché il carico è distribuito tra i computer client.
- Possono operare in ambienti con poca larghezza di banda perché la comunicazione tra agenti e server è ridotta.
- Sono ideali per i portatili. I computer verranno scansionati anche se il computer non è connesso alla rete aziendale.
- Sono più precise delle scansioni manuali, gli agenti possono accedere a maggiori informazioni sull'host locale.

La seguente schermata mostra in che modo è possibile distribuire le variabili di GFI LanGuard mediante agenti in una LAN (Local Area Network):

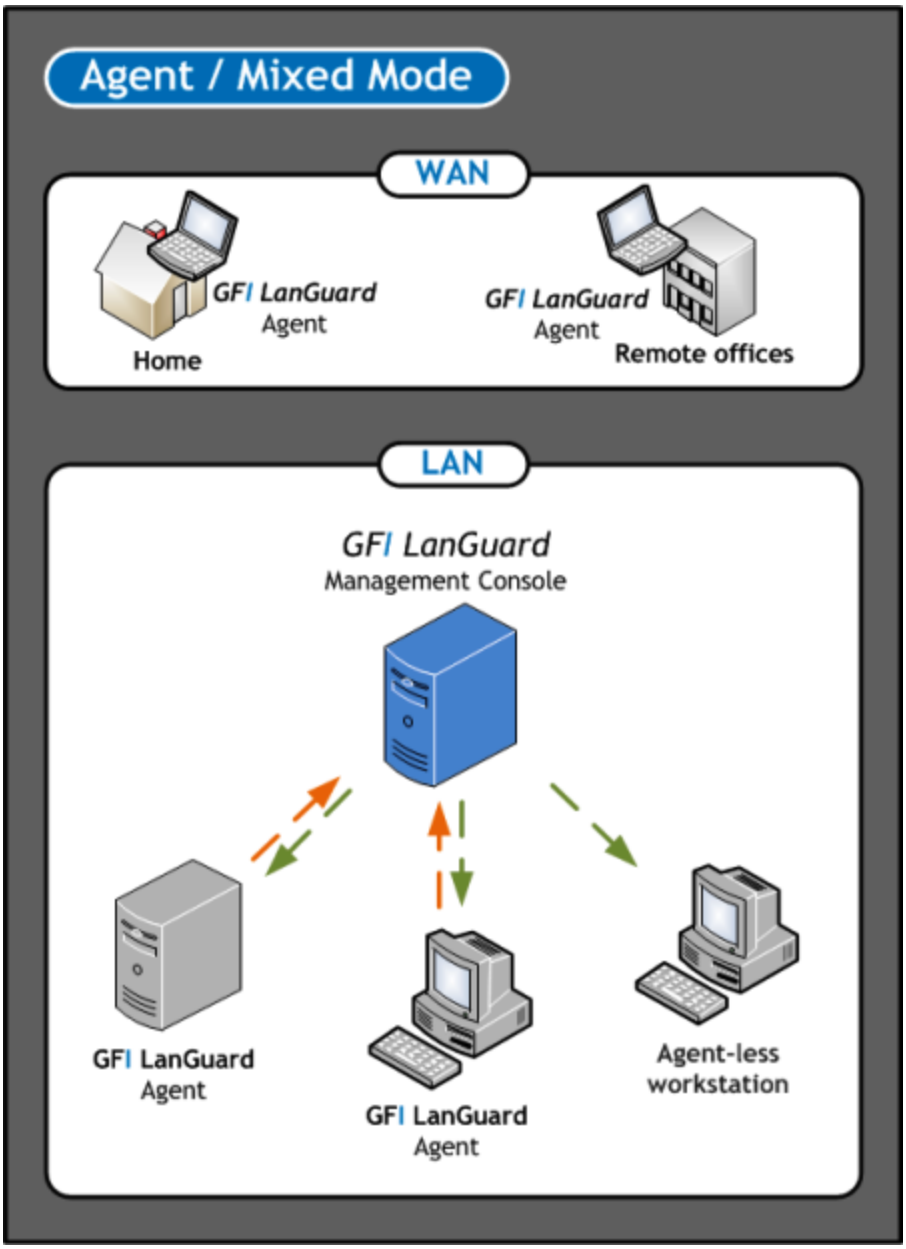


Figure 2: Modalità agente/mista

2.1.2 Distribuzione di GFI LanGuard con agenti relay

Gli agenti relay vengono utilizzati per ridurre il carico dal server GFI LanGuard. I computer configurati come agenti relay scaricheranno le patch e le definizioni direttamente dal server GFI LanGuard e le inoltreranno ai computer client. I vantaggi principali nell'utilizzo degli agenti relay includono:

- Risparmio della larghezza di banda della rete nelle reti locali o distribuite geograficamente. Se l'agente relay è configurato su ciascun lato, una patch viene scaricata una sola volta e distribuita ai client
- Il carico viene rimosso dal componente server di GFI LanGuard e distribuito negli agenti relay
- Poiché i computer vengono gestiti da più agenti relay, aumenta il numero di dispositivi che possono essere protetti contemporaneamente.

In una rete è possibile suddividere i computer in gruppi assegnare ciascun gruppo a un agente relay, come mostrato di seguito.

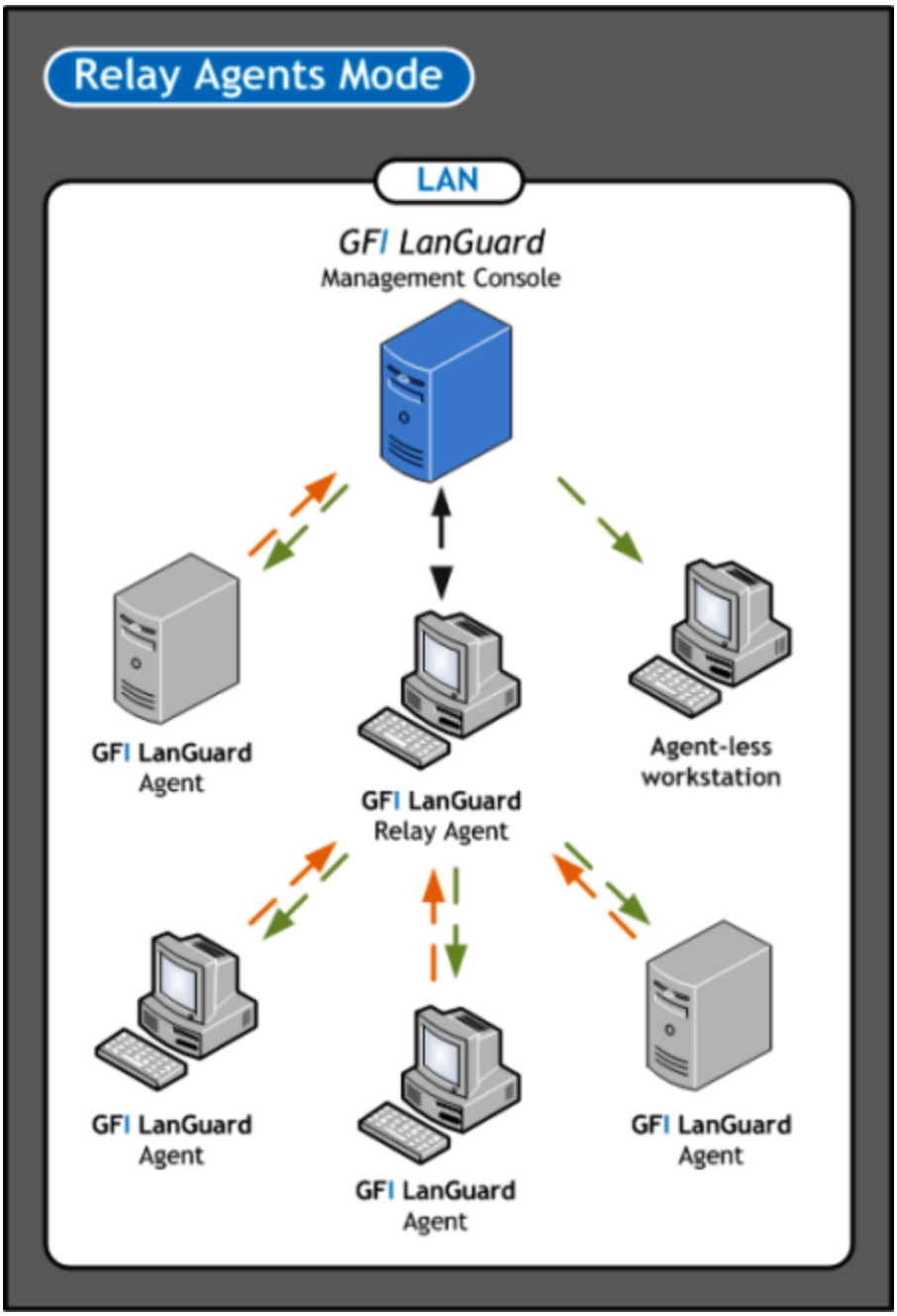


Figure 3: Modalità agente relay

> **Nota**
>
> For more information, refer to Configurazione degli agenti relay (page 54).

2.1.3 Distribuzione di GFI LanGuard in modalità senza agente

Il controllo senza agente viene avviato dalla console di gestione di GFI LanGuard. GFI LanGuard crea una sessione remota con le destinazioni di scansione specificate controllandole in rete. Al termine, i risultati vengono importati nel database relativo e la sessione remota viene terminata.

È possibile controllare singoli computer, una gamma di computer specifici e un intero dominio/gruppo di lavoro.

Nota

Le scansioni in modalità senza agente utilizzano le risorse del computer in cui è installato GFI LanGuard e impiegano una larghezza di banda della rete maggiore poiché il controllo viene eseguito in remoto. Se si dispone di una rete notevole di destinazioni di scansioni, questa modalità può diminuire considerevolmente le prestazioni di GFI LanGuard oltre a compromettere la velocità della rete. Nelle reti più grandi distribuire gli agenti/agenti relay in modo da bilanciare equamente il carico.

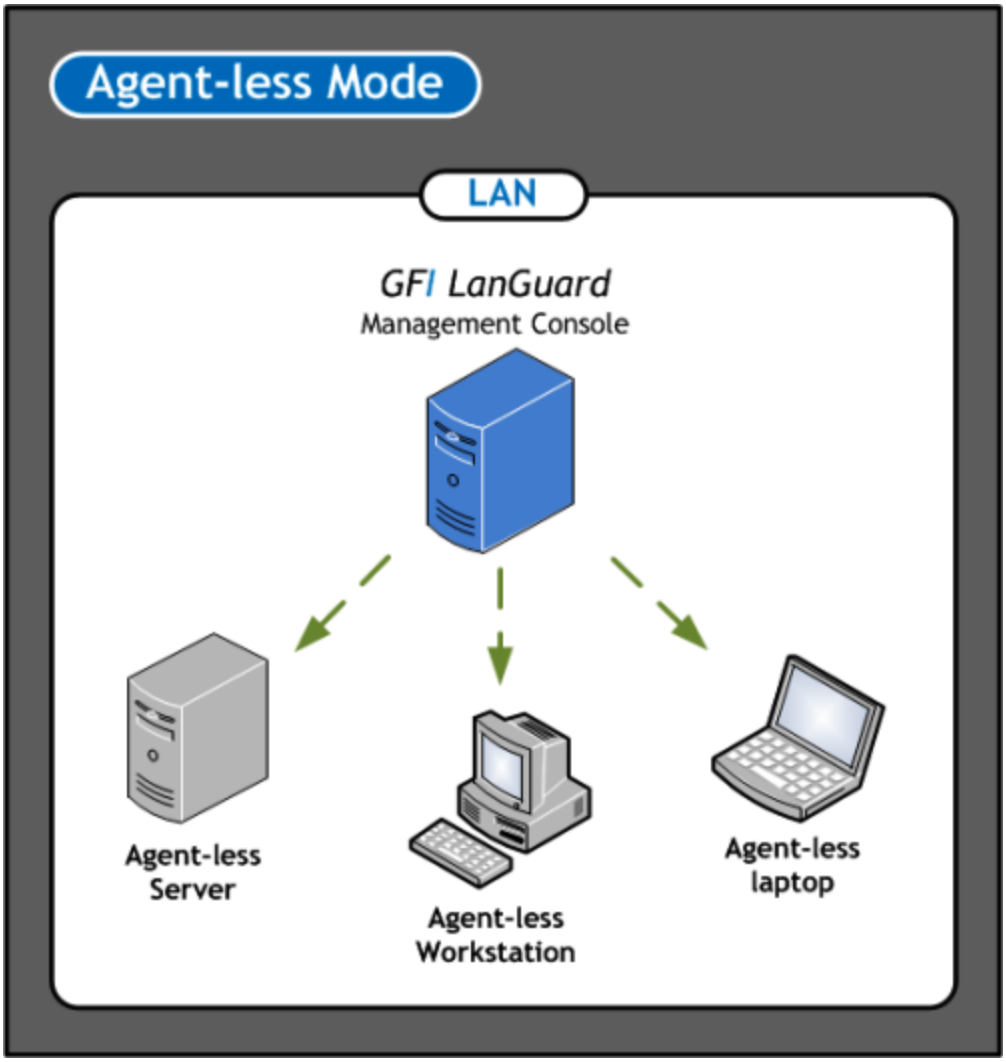


Figure 4: Modalità senza agente

2.2 Requisiti di sistema

Per garantire prestazioni eccellenti, i computer che eseguono il server/agente/agente relay GFI LanGuard devono soddisfare i requisiti di sistema descritti di seguito.

> **Nota**
>
> Se state cercando una soluzione di gestione patch per 2.000 o più computer, vi consigliamo di contattarci per i prezzi e altre indicazioni in merito alla corretta distribuzione e procedura di gestione per una soluzione simile.

Per ulteriori informazioni, fare riferimento alle seguenti sezioni:

- Requisiti hardware
- Requisiti software
- Porte firewall e protocolli
- Autorizzazioni gateway
- Applicazioni antivirus/antispyware supportate

2.2.1 Requisiti hardware

Assicurarsi che, per i computer che eseguono i componenti elencati di seguito, vengano soddisfatti i requisiti hardware specificati in basso:

- GFI LanGuardServer
- GFI LanGuardAgente
- GFI LanGuard Agente relay

GFI LanGuardServer

I computer che ospitano GFI LanGuard server devono soddisfare i requisiti hardware seguenti:

Table 3: Requisiti hardware - GFI LanGuard Server

Componente	Da 1 a 100 computer	Da 100 a 500 computer	Da 500 a 3.000 computer
Processore	2 GHz Dual Core	2.8 GHz Dual Core	3 GHz Quad Core
Archiviazione fisica	5 GB	10 GB	20 GB
RAM	2 GB	4 GB	8 GB
Larghezza di banda della rete	1544 Kbps	1544 Kbps	1544 Kbps

GFI LanGuardAgente

I computer che eseguono un agente GFI LanGuard devono soddisfare i requisiti hardware seguenti:

Table 4: Requisiti hardware - GFI LanGuard Agente

Componente	Requisiti
Processore	1 GHz
Archiviazione fisica	350 MB
RAM	25 MB
Larghezza di banda della rete	1544 Kbps

GFI LanGuard Agente relay

Un computer può essere configurato come agente relay quando:

- il computer è in linea con un buon tempo di attività
- Dispone di un accesso rapido ai computer connessi ad esso
- Dispone dello spazio su disco richiesto per consentire la memorizzazione nella cache.

I computer configurati come agente relay devono soddisfare i requisiti hardware seguenti:

Table 5: Requisiti hardware - GFI LanGuard Agente relay

Componente	Da 1 a 100 client	Da 100 a 500 client	Da 500 a 1.000 client
Processore	2 GHz Dual Core	2 GHz Dual Core	2.8 GHz Dual Core
Archiviazione fisica	5 GB	10 GB	10 GB
RAM	2 GB	2 GB	4 GB
Larghezza di banda della rete	100 Mbps	100 Mbps	1 Gbps

2.2.2 Requisiti software

I componenti GFI LanGuard possono essere installati in qualsiasi computer che soddisfi i requisiti software elencati in questa sezione. Per ulteriori informazioni, fare riferimento a:

- Sistemi operativi supportati
- Database supportati
- Componenti computer di destinazione
- Altri componenti software

Sistemi operativi supportati (32-bit/64-bit)

Nella tabella che segue vengono elencati i sistemi operativi in cui può essere installato GFI LanGuard server/agente/agente relay:

Table 6: Sistemi operativi supportati

Sistema operativo	GFI LanGuard	GFI LanGuardAgente	GFI LanGuard Agente relay
Windows® Server 2012	✓	✓	✓
Windows® Server 2008 (incluso R2) Standard/Enterprise	✓	✓	✓
Windows®Server 2003 Standard/Enterprise	✓	✓	✓
Windows® 8	✓	✓	✓
Windows® 7 Professional/Enterprise/Ultimate	✓	✓	✓
Windows® Vista Business/Enterprise/Ultimate	✓	✓	✓
Windows® XP Professional (SP2 o versioni successive)	✓	✓	✓
Windows® Small Business Server 2008 Standard	✓	✓	✓
Windows® Small Business Server 2003 (SP1)	✓	✓	✓

Sistema operativo	GFI LanGuard	GFI LanGuardAgente	GFI LanGuard Agente relay
Windows® 2000 Professional/Server/Advanced » SP4 » Internet Explorer 6 SP1 o versioni successive » Windows Installer 3.1 o versioni successive	✗	✓	✓

Database supportati

GFI LanGuard utilizza un database per archiviare le informazioni dai controlli di sicurezza della rete e dalle operazioni di riparazione. Il back-end database può essere uno dei seguenti componenti:

Table 7: Database back-end supportati

Database	Uso consigliato
Microsoft ® Access	Consigliato per la valutazione e per un massimo di 5 computer.
Edizione MSDE/SQL Server Express®.	Consigliato per le reti con un massimo di 500 computer.
SQL Server® 2000 o versione successiva	Consigliato per reti più grandi con 500 computer o oltre.

Componenti computer di destinazione

Nella tabella che segue vengono fornite le informazioni sui componenti necessari per essere installati/abilitati sui computer da sottoporre a scansione in remoto da GFI LanGuard:

Table 8: Requisiti software - Componenti aggiuntivi

Componente	Descrizione
Secure Shell (SSH)	obbligatoria per le destinazioni di scansione basate su UNIX. Normalmente incluso in tutte le principali distribuzioni Unix/Linux.
Strumentazione gestione Windows (WMI)	obbligatoria per la scansione delle destinazioni di scansione basate su Windows. Presente in tutti i sistemi operativi con Windows 2000 o più recenti.
Condivisione file e stampanti	obbligatoria per enumerare e raccogliere le informazioni sulle destinazioni di scansione.
Registro di sistema remoto	obbligatorio per GFI LanGuard per eseguire un servizio temporaneo per la scansione di una destinazione remota.

Componenti GFI LanGuard server aggiuntivi

Il componente seguente è obbligatorio per il computer in cui è installato il componente server GFI LanGuard:

» Microsoft .NET® Framework 3.5

2.2.3 Porte firewall e protocolli

Nella sezione seguente vengono fornite le informazioni sulle impostazioni di protocolli e porte firewall obbligatori:

» GFI LanGuard Server e agenti relay

» GFI LanGuard Computer agente e senza agente

GFI LanGuard e agenti relay

Configurare il firewall per consentire le connessioni **In entrata** sulla porta TCP **1070** nei computer che eseguono:

» GFI LanGuard

» Agenti relay

Questa porta viene utilizzata automaticamente quando è installato GFI LanGuard e gestisce tutta la comunicazione in entrata tra il componente server e i computer monitorati. Se GFI LanGuard rileva che la porta 1070 è già in uso da un'altra applicazione, ricerca automaticamente una porta disponibile nell'intervallo **1070-1170**.

Per configurare manualmente la porta di comunicazione:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Configurazione> Gestione agenti**.

3. Dal riquadro di destra fare clic su **Impostazioni agenti**.

4. Dalla finestra di dialogo **Impostazioni agenti** specificare la porta di comunicazione nella casella di testo **Porta TCP**.

5. Fare clic su **OK**.

GFI LanGuard Computer agente e senza agente

GFI LanGuard comunica con i computer gestiti (agenti e senza agente), utilizzando le porte e i protocolli seguenti. Il firewall dei computer gestiti deve essere configurato per consentire le richieste **In entrata** sulle porte:

Table 9: Porte e protocolli

Porte TCP	Protocollo	Descrizione
22	SSH	Controllo sistemi operativi Linux in corso.
135	DCOM	Porta assegnata in modo dinamico.
137	NetBIOS	Individuazione dei computer e condivisione di risorse.
138	NetBIOS	Individuazione dei computer e condivisione di risorse.
139	NetBIOS	Individuazione dei computer e condivisione di risorse.
161	SNMP	Individuazione dei computer.
445	SMB	Utilizzato durante: » controllo dei computer » gestione degli agenti » Distribuzione delle patch.

2.2.4 Autorizzazioni gateway

Per scaricare gli aggiornamenti delle definizioni e di sicurezza, GFI LanGuard si connette ai server di aggiornamento di GFI, di Microsoft e di terze parti tramite HTTP. Assicurarsi che il computer dove è installato GFI LanGuard consenta le connessioni a:

- *software.gfi.com/lnsupdate/
- *.download.microsoft.com
- *.windowsupdate.com
- *.update.microsoft.com
- Tutti i server di aggiornamento dei fornitori di terze parti supportati da GFI LanGuard.

Nota

Per ulteriori informazioni, fare riferimento a:

- Applicazioni supportate di terze parti:
  - http://go.gfi.com/?pageid=LAN_PatchMng
- Bollettini di applicazioni supportate:
  - http://go.gfi.com/?pageid=3p_fullreport
- Applicazioni Microsoft supportate:
  - http://go.gfi.com/?pageid=ms_app_fullreport
- Bollettini Microsoft supportati:
  - http://go.gfi.com/?pageid=ms_fullreport

2.2.5 Applicazioni antivirus/antispyware supportate

GFI LanGuard rileva i file di definizione scaduti di una serie di software antivirus e antispyware. Per un elenco completo del software antivirus e antispyware supportato, consultare: http://go.gfi.com/?pageid=security_app_fullreport

2.3 Importazione ed esportazione delle impostazioni

GFI LanGuard consente di importare ed esportare le impostazioni. Le impostazioni che è possibile importare/esportare comprendono:

- Profili di scansione
- Valutazione delle vulnerabilità
- porte (TCP/UDP)
- rapporti di filtraggio risultati
- impostazioni di riparazione automatica (disinstallazione automatica e impostazioni delle patch)
- opzioni (database back-end, avviso, scansione pianificata e impostazioni interne)

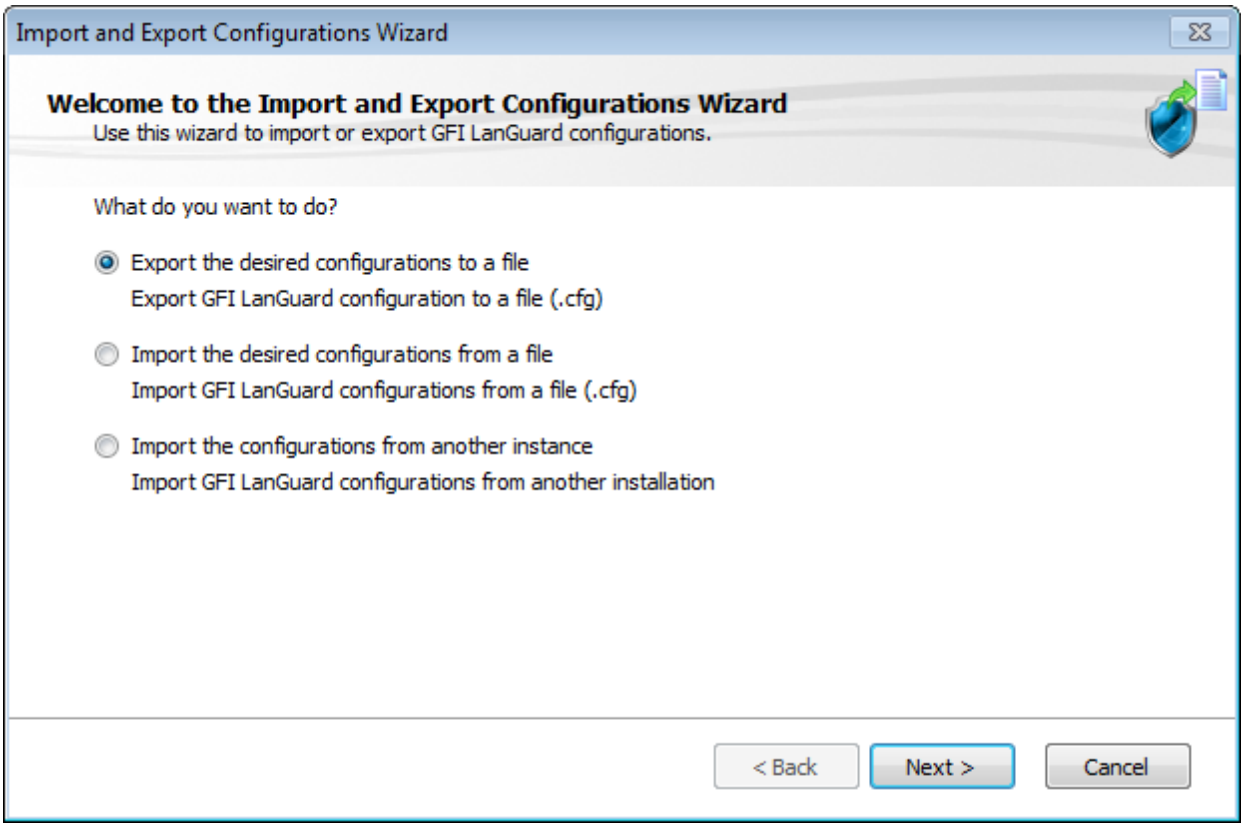
Le seguenti sezioni contengono informazioni relative a:

- Esportazione delle configurazioni in un file
- Importazione configurazioni da file
- Importazione delle configurazioni desiderate da un'altra istanza di GFI LanGuard.

2.3.1 Esportazione delle configurazioni in un file

Per esportare le configurazioni:

1. Avviare GFI LanGuard.
2. Fare clic sul **GFI LanGuardpulsante> File > Importa ed esporta configurazioni…**
3. Selezionare **Esporta la configurazione desiderata in un file** e fare clic su **Avanti**.
4. Specificare il percorso in cui salvare la configurazione esportata e fare clic su **Avanti**.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
Use this wizard to import or export GFI LanGuard configurations.
What do you want to do?
Export the desired configurations to a file
Export GFI LanGuard configuration to a file (.cfg)
Import the desired configurations from a file
Import GFI LanGuard configurations from a file (.cfg)
Import the configurations from another instance
Import GFI LanGuard configurations from another installation
< Back
Next >
Cancel

Screenshot 1: Esportazione configurazioni in un file

5. Attendere il caricamento della struttura della configurazione e selezionare le configurazioni da esportare. Fare clic su **Avanti** per avviare l'esportazione.

6. Una finestra di dialogo di notifica confermerà il completamento dell'esportazione.

7. Fare clic su **OK** per uscire dall'applicazione.

2.3.2 Importazione configurazioni da file

Per importare le configurazioni salvate:

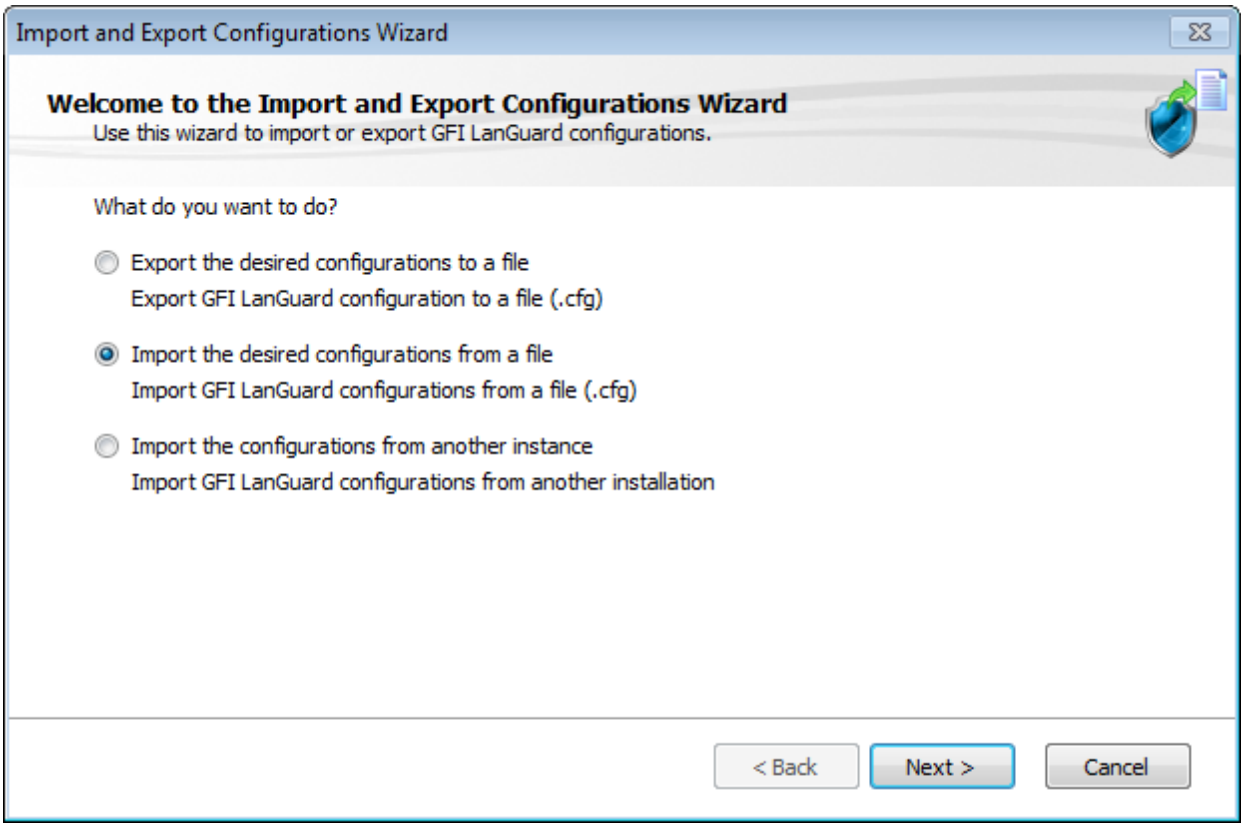
1. Avviare GFI LanGuard.

2. Fare clic sul **GFI LanGuard pulsante > File > Importa ed esporta configurazioni…**

3. Selezionare Importa la configurazione desiderata da un file e fare clic su **Avanti**.

4. Specificare il percorso dal quale caricare la configurazione e fare clic su **Avanti**.

5. Attendere il caricamento della struttura della configurazione e selezionare le configurazioni da importare. Fare clic su **Avanti** per avviare l'importazione.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
Use this wizard to import or export GFI LanGuard configurations.
What do you want to do?
Export the desired configurations to a file
Export GFI LanGuard configuration to a file (.cfg)
Import the desired configurations from a file
Import GFI LanGuard configurations from a file (.cfg)
Import the configurations from another instance
Import GFI LanGuard configurations from another installation
< Back
Next >
Cancel

Screenshot 2: Importazione configurazioni da file

6. Nella finestra di dialogo visualizzata, confermare o meno l'operazione di sovrascrittura facendo clic su **Sì** o **No**.

7. Una finestra di dialogo di notifica confermerà il completamento dell'esportazione.

8. Fare clic su **OK** per uscire dall'applicazione.

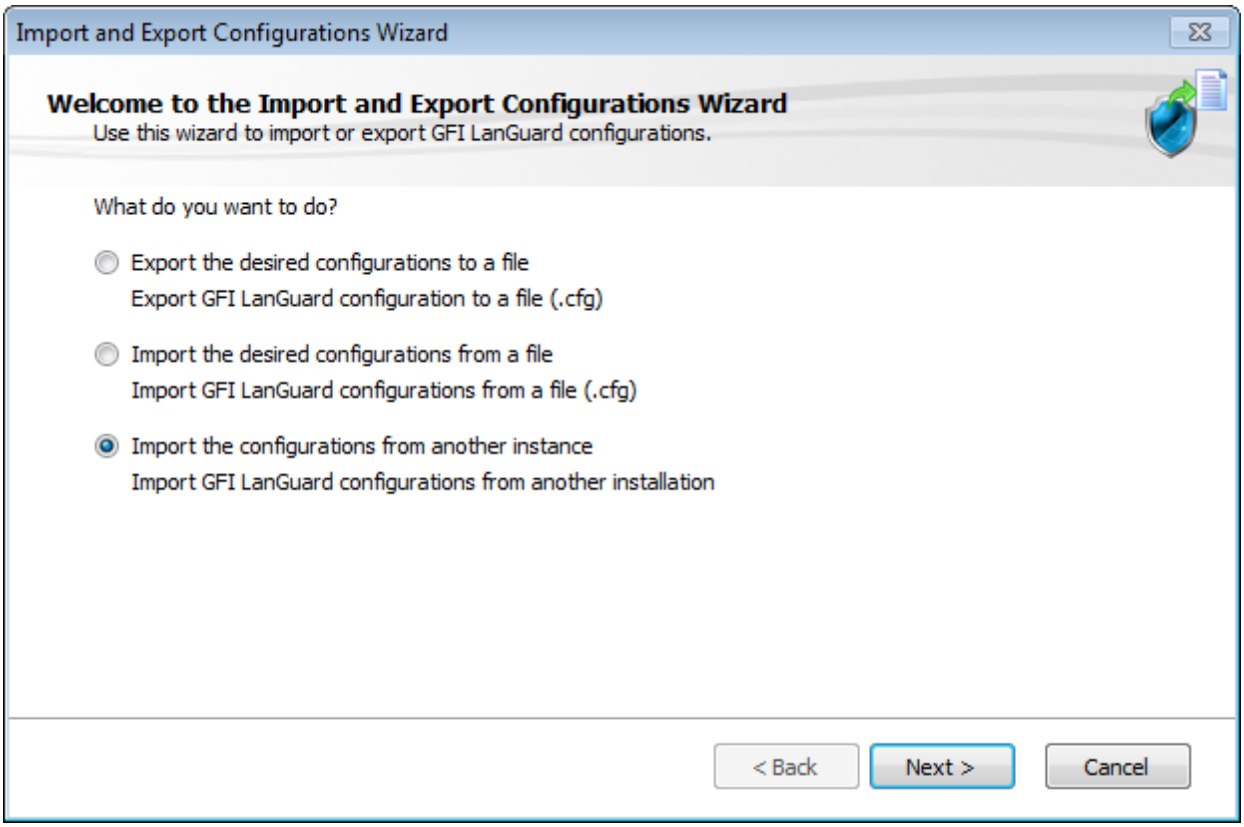
2.3.3 Importazione delle configurazioni desiderate da un'altra istanza di GFI LanGuard.

1. Avviare GFI LanGuard.

2. Fare clic sul pulsante **GFI LanGuard > File > Importa ed esporta configurazioni...** per avviare la **procedura guidata Importa ed esporta configurazioni**.

3. Selezionare **Importa le configurazioni desiderate da un'altra istanza**, quindi fare clic su **Avanti**.

4. Per selezionare la cartella di installazione di GFI LanGuard, fare clic su **Sfoglia**. La posizione predefinita è `<Disco locale>\Programmi\GFI\ LanGuard <Versione>`. Fare clic su **Avanti**.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
Use this wizard to import or export GFI LanGuard configurations.
What do you want to do?
Export the desired configurations to a file
Export GFI LanGuard configuration to a file (.cfg)
Import the desired configurations from a file
Import GFI LanGuard configurations from a file (.cfg)
Import the configurations from another instance
Import GFI LanGuard configurations from another installation
< Back
Next >
Cancel

Screenshot 3: Importazione impostazione

5. Selezionare le impostazioni da importare e fare clic su **Avanti**.

6. Durante l'importazione, GFI LanGuard chiederà all'utente se desidera sostituire o mantenere le impostazioni correnti. Selezionare una delle seguenti opzioni:

Table 10: Opzioni di sostituzione

Opzione	Descrizione
Sì	Sostituisce l'impostazione corrente con quella importata.
No	Mantiene l'impostazione corrente e ignora quella importata.
Rinomina˚automaticamente	Rinomina le impostazioni importate e mantiene quelle attuali.

7. Quando l'importazione è pronta, fare clic su **OK**.

2.4 Aggiornamento da versioni precedenti

GFI LanGuard conserva tutte le impostazioni e le informazioni sui risultati di qualsiasi versione precedente di GFI LanGuard. Ciò consente di:

- Installare GFI LanGuard senza disinstallare la versione precedente.
- Importare in GFI LanGuard le impostazioni di altre istanze.
- Distribuire agenti negli stessi computer dove è installata una versione precedente di GFI LanGuard.

> **Nota**
>
> Non è possibile effettuare aggiornamento software da versioni precedenti a GFI LanGuard 9.

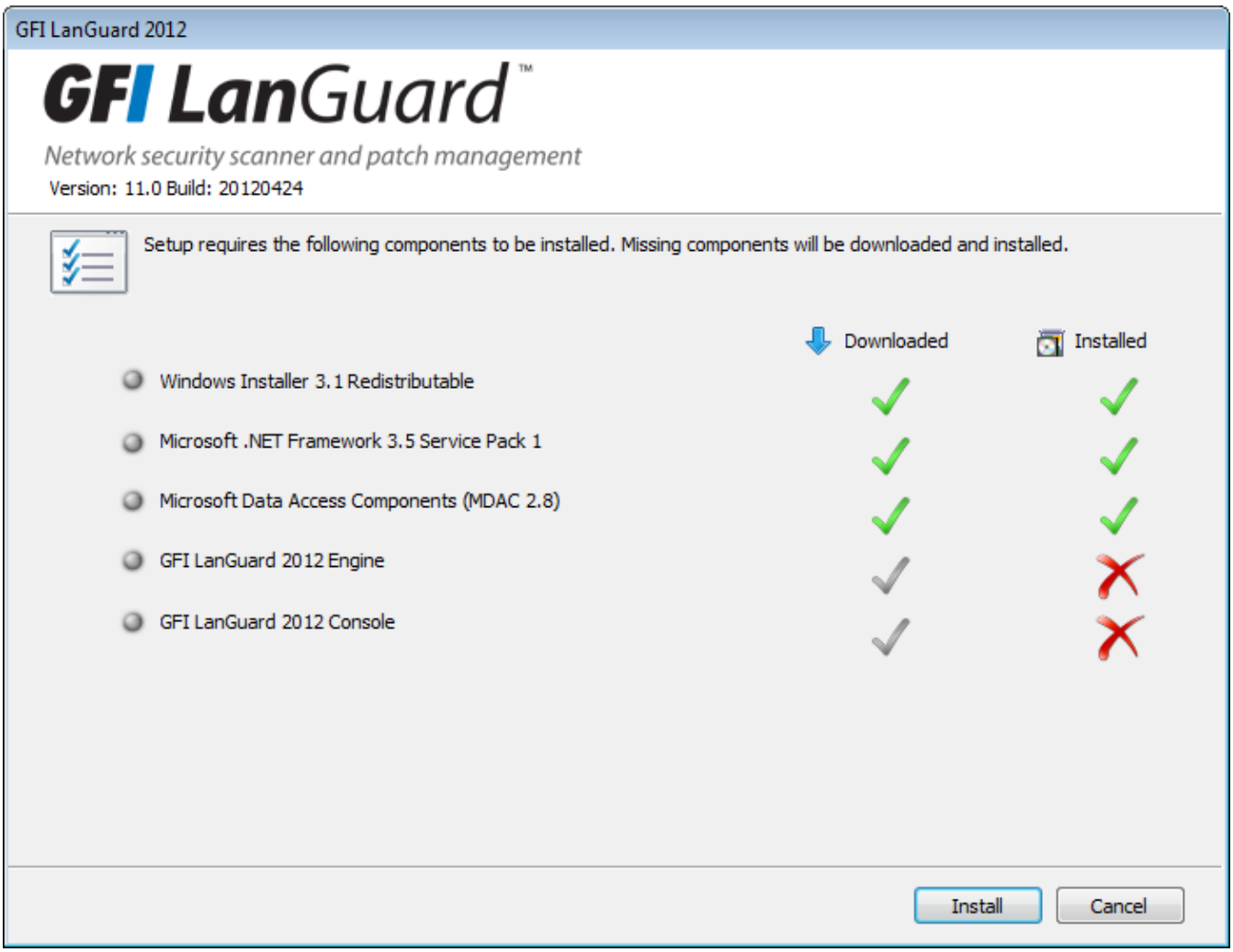
Nota

I codici di licenza delle versioni precedenti di GFI LanGuard non sono compatibili e devono essere aggiornati per poter eseguire GFI LanGuard.

Per eseguire l'aggiornamento a una versione più recente:

1. Accedere al computer dove sarà installato GFI LanGuard utilizzando le credenziali dell'amministratore.

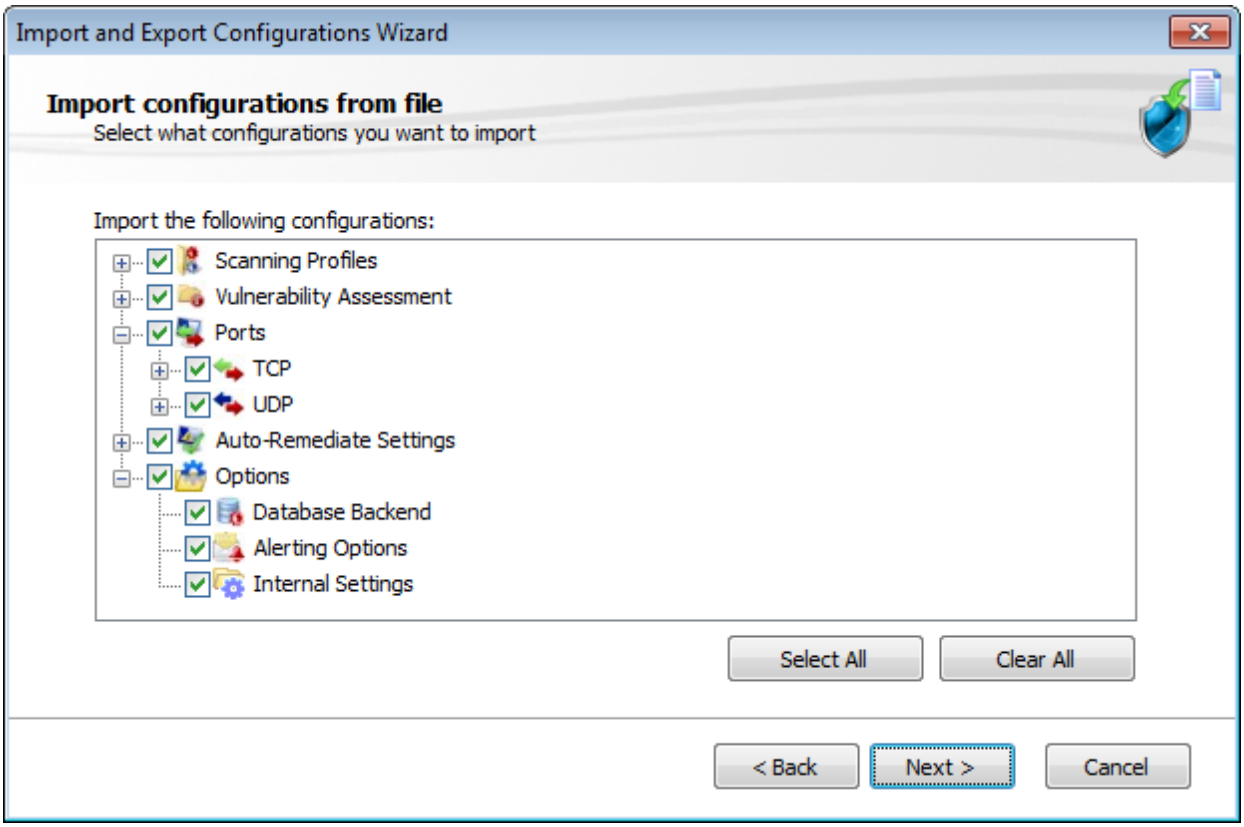
2. Avviare l'installazione di GFI LanGuard.


GFI LanGuard 2012
GFI LanGuard
Network security scanner and patch management
Version: 11.0 Build: 20120424
Setup requires the following components to be installed. Missing components will be downloaded and installed.
Downloaded
Installed
Windows Installer 3.1 Redistributable
Microsoft .NET Framework 3.5 Service Pack 1
Microsoft Data Access Components (MDAC 2.8)
GFI LanGuard 2012 Engine
GFI LanGuard 2012 Console
Install
Cancel

Screenshot 4: Finestra di dialogo Controllo prerequisiti

3. La finestra di dialogo del controllo prerequisiti visualizza una panoramica dello stato dei componenti necessari al funzionamento di GFI LanGuard. Per avviare l'installazione, fare clic su **Installa**.

4. Per completare l'aggiornamento, seguire le istruzioni su schermo.



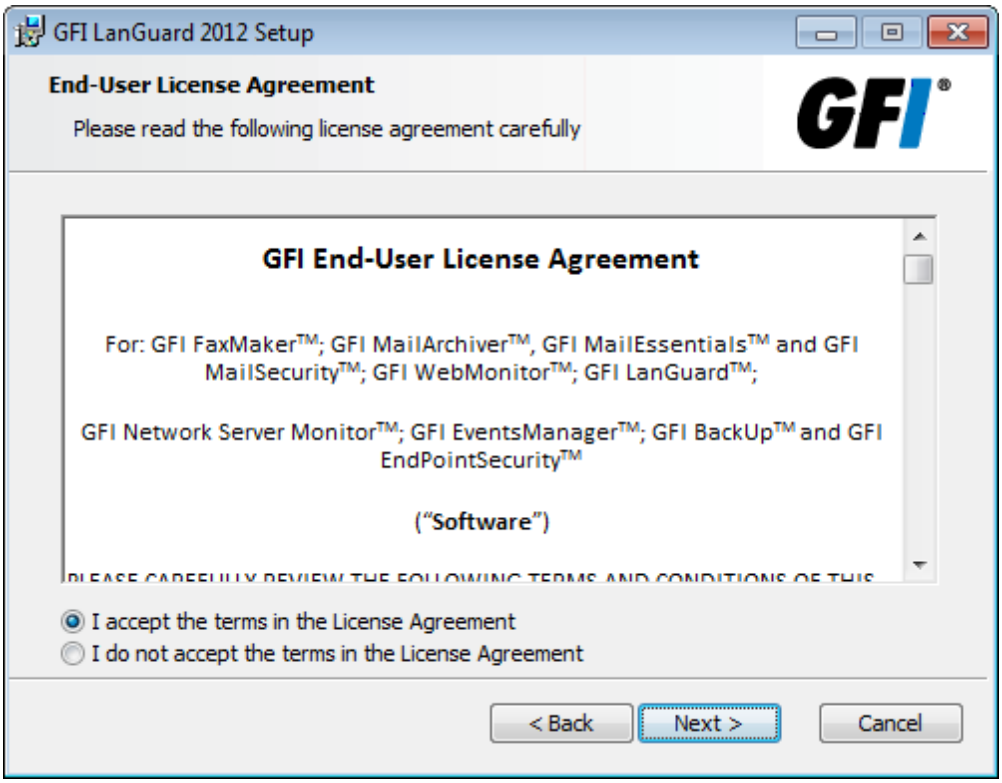
Screenshot 5: Importazione ed esportazione delle impostazioni di un'istanza precedente

5. Una volta installato GFI LanGuard, il programma rileva l'installazione precedente e avvia in automatico la **procedura guidata Importa ed esporta configurazioni**. Ciò consente l'esportazione delle varie configurazioni dalla versione precedente e la successiva importazione in una nuova.

6. Selezionare le configurazioni da importare e quindi fare clic su **Avanti** per finalizzare la procedura.

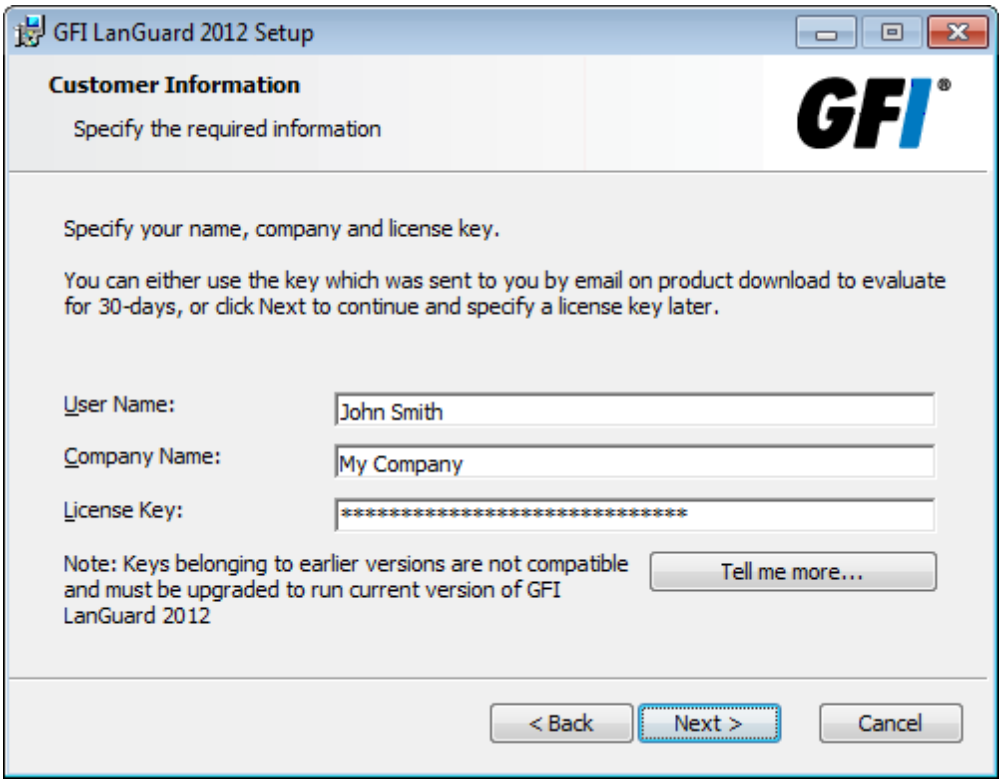
2.5 Nuova installazione

1. Accedere al computer dove sarà installato GFI LanGuard utilizzando le credenziali dell'amministratore.
2. Avviare l'installazione di GFI LanGuard.
3. Nella finestra di controllo prerequisito, fare clic su **Installa** per scaricare e installare eventuali componenti necessari.
4. Nella schermata di benvenuto di GFI LanGuard, fare clic su **Avanti** per procedere.


GFI LanGuard 2012 Setup
End-User License Agreement
Please read the following license agreement carefully
GFI End-User License Agreement
For: GFI FaxMaker™; GFI MailArchiver™, GFI MailEssentials™ and GFI MailSecurity™; GFI WebMonitor™; GFI LanGuard™;
GFI Network Server Monitor™; GFI EventsManager™; GFI BackUp™ and GFI EndPointSecurity™
("Software")
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
< Back
Next >
Cancel

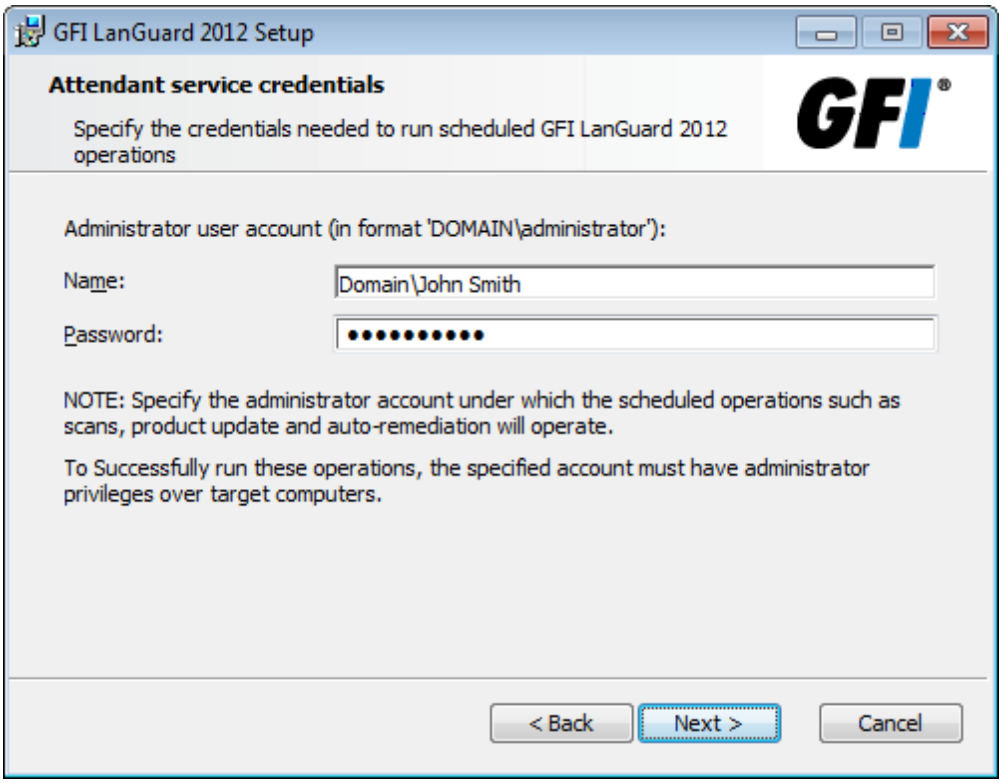
Screenshot 6: Contratto di licenza con l'utente finale

5. Leggere attentamente il contratto di licenza. Per procedere con l'installazione, selezionare **Accetto i termini del contratto di licenza** e fare clic su **Avanti**.


GFI LanGuard 2012 Setup
Customer Information
Specify the required information
Specify your name, company and license key.
You can either use the key which was sent to you by email on product download to evaluate for 30-days, or click Next to continue and specify a license key later.
User Name:
John Smith
Company Name:
My Company
License Key:
Note: Keys belonging to earlier versions are not compatible and must be upgraded to run current version of GFI LanGuard 2012
Tell me more...
< Back
Next >
Cancel

Screenshot 7: Specifica dei dati dell'utente e della chiave di licenza

6. Specificare i dati dell'utente e inserire la chiave di licenza relativa. Fare clic su **Avanti**.


GFI LanGuard 2012 Setup
Attendant service credentials
Specify the credentials needed to run scheduled GFI LanGuard 2012 operations
GFI
Administrator user account (in format 'DOMAIN\administrator'):
Name:
Domain\John Smith
Password:
NOTE: Specify the administrator account under which the scheduled operations such as scans, product update and auto-remediation will operate.
To Successfully run these operations, the specified account must have administrator privileges over target computers.
< Back
Next >
Cancel

Screenshot 8: Credenziali servizio attendant

7. Digitare le credenziali dell'amministratore e la password. Verranno utilizzate dal servizio che eseguirà le operazioni pianificate. Per continuare l'installazione, fare clic su **Avanti**.
8. Fare clic su **Installa** per installare GFI LanGuard nella posizione predefinita o fare clic su **Sfoglia** per modificare il percorso.
9. Per completare l'installazione, fare clic su **Fine**.

Al primo avvio, GFI LanGuard abilita in automatico il controllo sul computer locale e lo scansiona alla ricerca di vulnerabilità. Una volta completata tale procedura, la pagina **Home** di GFI LanGuard visualizza il risultato delle vulnerabilità.

Nota

È necessaria la connessione a Internet per scaricare i componenti mancanti.

Nota

Se le credenziali non sono valide, verrà visualizzato un messaggio che indica la possibilità di ignorare questa opzione. Si consiglia di inserire un nome utente e password validi e di non ignorare questa opzione.

Nota

Utilizzare il database di Microsoft Access solo se si sta valutando GFI LanGuard e si usano fino a 5 computer. Per ulteriori informazioni, fare riferimento alla sezione Configurazione opzioni di manutenzione database.

Nota

Una volta installato il prodotto, eseguire una verifica dell'installazione. For more information, refer to Verifica dell'installazione (page 37).

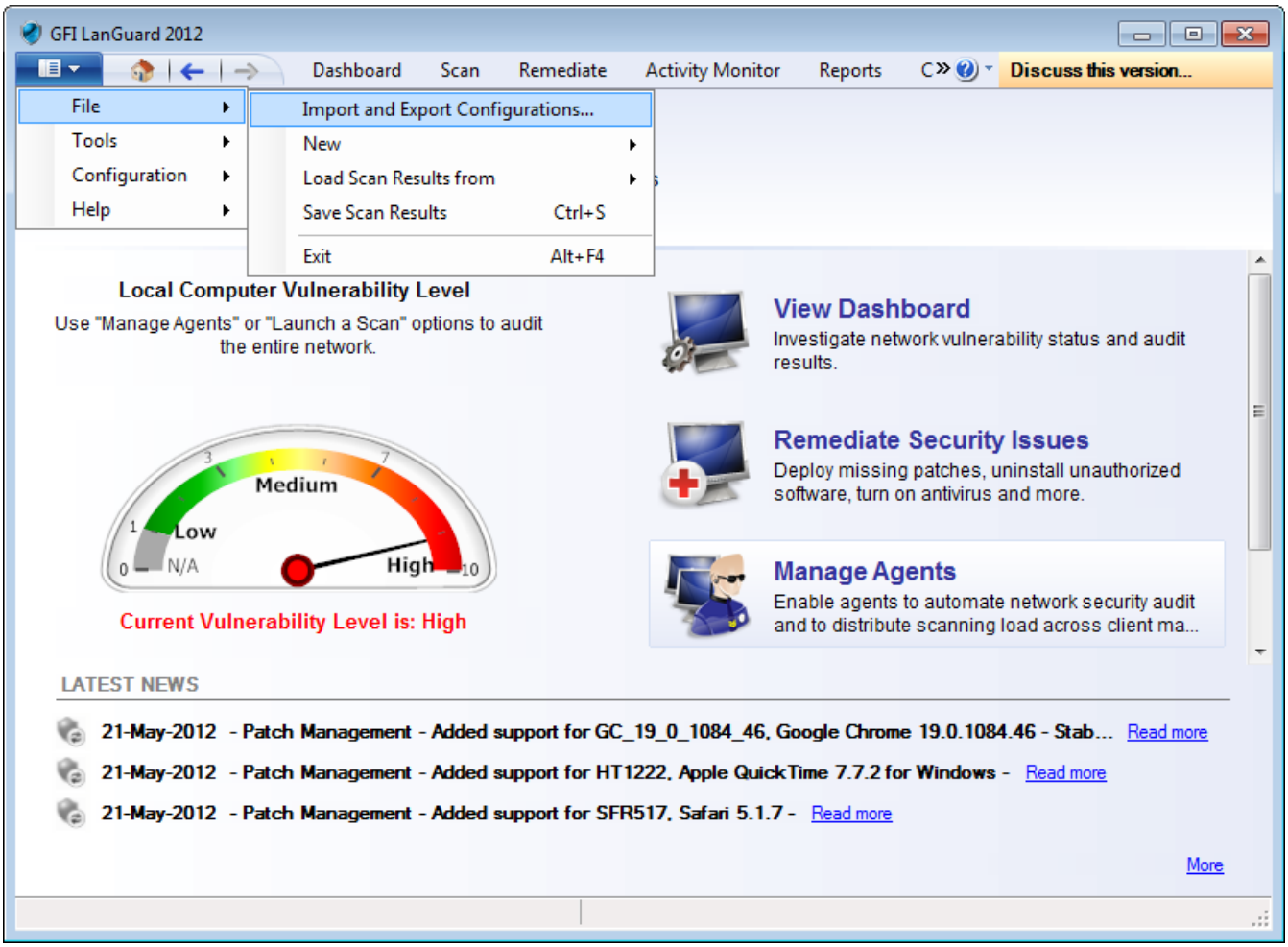
2.6 Azioni post-installazione

GFI LanGuard può essere installato in un computer con una versione precedente di GFI LanGuard senza necessità di disinstallare questa versione. In questo modo verranno mantenute le impostazioni di configurazione e verranno riutilizzate nella nuova versione.

Per importare le impostazioni da una versione precedente:

1. Avviare la console di gestione di GFI LanGuard da **Start > Tutti i programmi > GFI LanGuard 2012 > GFI LanGuard 2012**.

2. Fare clic sul pulsante **GFI LanGuard > File > Importa ed esporta configurazioni…** per avviare la **procedura guidata Importa ed esporta configurazioni**.


GFI LanGuard 2012
Dashboard
Scan
Remediate
Activity Monitor
Reports
Discuss this version...
File
Tools
Configuration
Help
Import and Export Configurations...
New
Load Scan Results from
Save Scan Results Ctrl+S
Exit Alt+F4
Local Computer Vulnerability Level
Use "Manage Agents" or "Launch a Scan" options to audit the entire network.
Medium
Low
High
N/A
Current Vulnerability Level is: High
View Dashboard
Investigate network vulnerability status and audit results.
Remediate Security Issues
Deploy missing patches, uninstall unauthorized software, turn on antivirus and more.
Manage Agents
Enable agents to automate network security audit and to distribute scanning load across client ma...
LATEST NEWS
21-May-2012 - Patch Management - Added support for GC_19_0_1084_46, Google Chrome 19.0.1084.46 - Stab... Read more
21-May-2012 - Patch Management - Added support for HT1222, Apple QuickTime 7.7.2 for Windows - Read more
21-May-2012 - Patch Management - Added support for SFR517, Safari 5.1.7 - Read more
More

Screenshot 9: Importazione ed esportazione configurazioni

3. Selezionare **Importa le configurazioni desiderate da un'altra istanza**, quindi fare clic su **Avanti**.

4. Per selezionare la cartella di installazione di GFI LanGuard, fare clic su **Sfoglia**. Il percorso predefinito è:

- **Computer a 64 bit (x64)** - `<Disco locale>\Programmi (x86)\GFI\ LanGuard <Versione>`
- **Computer a 32 bit (x86)** - `<Disco locale>\Programmi\GFI\ LanGuard <Versione>`

5. Fare clic su **Avanti**.

6. Selezionare le impostazioni da importare, quindi fare clic su **Avanti**.

7. Durante l'importazione, GFI LanGuard chiederà all'utente se desidera sostituire o mantenere le impostazioni correnti. Selezionare:

Table 11: Opzioni di sostituzione di importazione

Opzione	Descrizione
Sì	Sostituisce l'impostazione corrente con quella importata.
No	Mantiene l'impostazione corrente e ignora quella importata.
Rinomina automaticamente	Rinomina le impostazioni correnti e mantiene quelle attuali.

8. Al termine, fare clic su **OK**.

2.7 Verifica dell'installazione

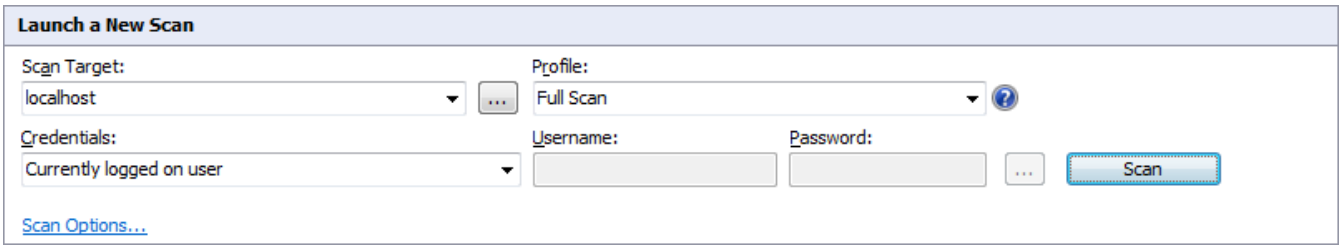
Una volta installato GFI LanGuard, verificare l'installazione eseguendo una scansione locale per assicurare che l'installazione sia andata a buon fine.

1. Avviare GFI LanGuard.

GFI LanGuard 2012
Dashboard
Scan
Remediate
Activity Monitor
Reports
Discuss this version...
Welcome to GFI LanGuard 2012
GFI LanGuard 2012 is ready to audit your network for vulnerabilities
Medium
Low
High
N/A
Current Vulnerability Level is: High
Remediate Security Issues
Deploy missing patches, uninstall unauthorized software, turn on antivirus and more.
Manage Agents
Enable agents to automate network security audit and to distribute scanning load across client ma...
Launch a Scan
Manually set-up and trigger an agentless network security audit.
LATEST NEWS
21-May-2012 - Patch Management - Added support for GC_19_0_1084_46, Google Chrome 19.0.1084.46 - Stab... Read more
21-May-2012 - Patch Management - Added support for HT1222, Apple QuickTime 7.7.2 for Windows - Read more
21-May-2012 - Patch Management - Added support for SFR517, Safari 5.1.7 - Read more
More

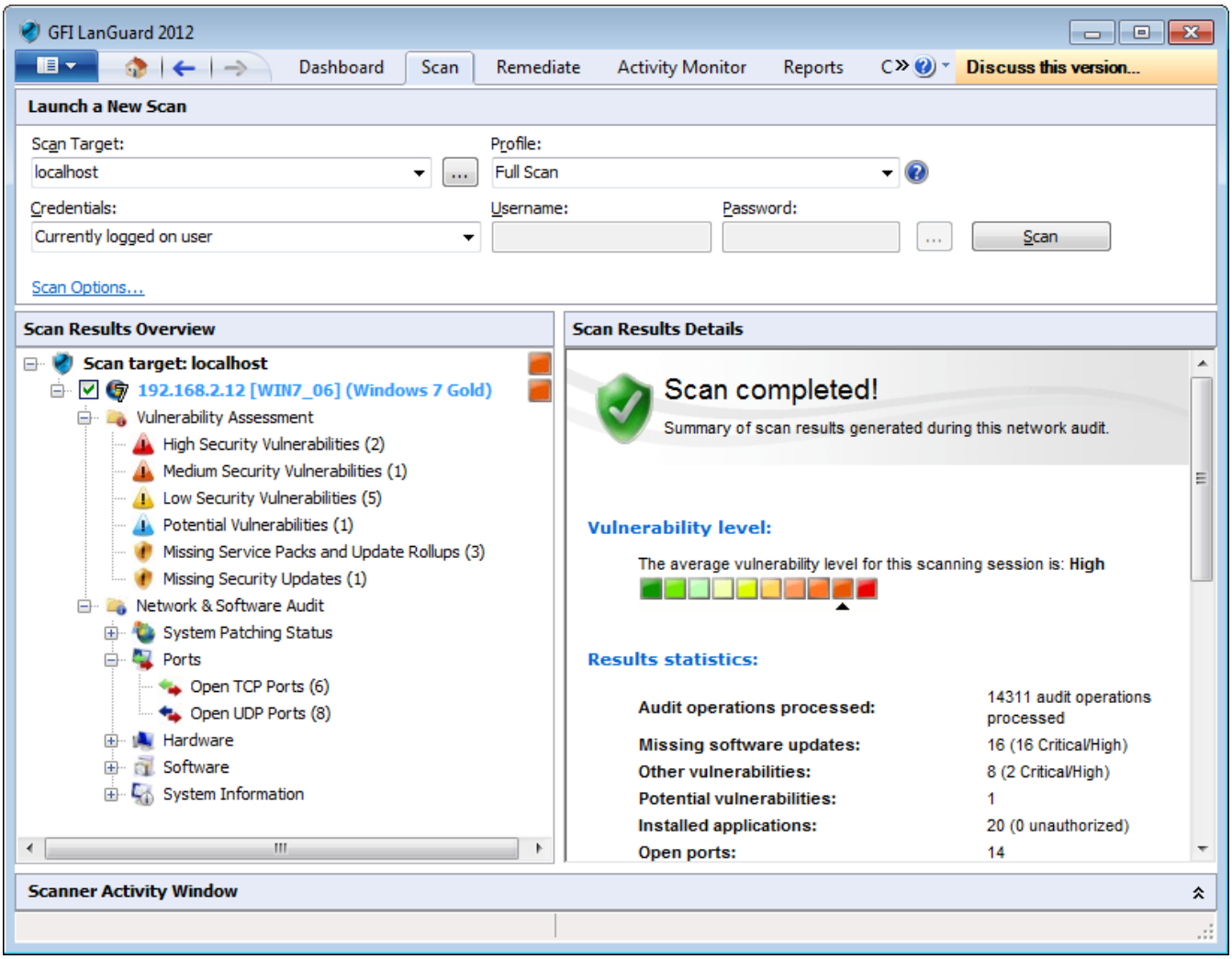
Screenshot 10: Avvia una scansione

2. Dalla homepage di GFI LanGuard, fare clic su **Avvia una scansione**.



Screenshot 11: Proprietà di Avvia una scansione

3. Dal menu a discesa **Scansiona destinazione**, selezionare **localhost**.
4. Dal menu a discesa **Profilo**, selezionare **Scansione completa**.
5. Per iniziare la scansione del computer locale, fare clic su **Scansiona**.
6. L'avanzamento della scansione viene visualizzato nella scheda **Scansiona**.



Screenshot 12: Riepilogo risultati di scansione

7. Al termine dell'operazione, la sezione **Avanzamento** riporterà una panoramica dei risultati di scansione.

8. Utilizzare le sezioni **Dettagli risultati di scansione** e **Panoramica risultati di scansione** per analizzare il risultato della scansione. For more information, refer to Interpretazione risultati scansione manuale (page 107).

3 Ottenere risultati

In questa sezione vengono fornite le istruzioni dettagliate su come irrobustire la sicurezza e l'integrità della rete utilizzando GFI LanGuard. Questa sezione aiuta a realizzare in modo positivo la gestione delle patch, la gestione della vulnerabilità e i risultati di conformità legale, avendo nel contempo la certezza di utilizzare le tecniche di detenzione delle vulnerabilità più aggiornate.

Argomenti del presente capitolo:

3.1 Valutazione efficace delle vulnerabilità 39
3.2 Gestione efficace delle patch 40
3.3 Utilizzo di GFI LanGuard per la tracciabilità asset 41
3.4 Analisi di rete e software aggiornata 42
3.5 Conformità a PCI DSS 43

3.1 Valutazione efficace delle vulnerabilità

Per un'efficace strategia di gestione delle vulnerabilità, seguire i passaggi sottostanti:

1. Mantenere aggiornato GFI LanGuard.

- Assicurarsi che il computer dove è installato GFI LanGuard disponga di accesso a Internet. GFI LanGuard Effettua controlli giornalieri alla ricerca di informazioni aggiornate.
- Se viene utilizzato un server proxy, fare riferimento alla sezione Configurazione impostazioni proxy.
- Se l'accesso a Internet non è disponibile sul computer dove è installato GFI LanGuard, fare riferimento alla sezione Installazione manuale degli aggiornamenti del programma.

2. Effettuare controlli di sicurezza regolari.

- Scansioni pianificate agente
- Scansioni manuali
- Scansioni pianificate

3. Distribuire gli aggiornamenti di sicurezza mancanti e rimuovere le applicazioni non autorizzate.

- Configurazione riparazione automatica agenti
- Configurazione riparazione automatica
- Distribuzione di patch di sicurezza e service pack
- Disinstallazione patch software e service pack

4. Investigare e riparare altri problemi di sicurezza.

- Distribuzione software personalizzato
- Operazioni di protezione antimalware
- Disinstallazione delle applicazioni personalizzate
- Utilizzo del supporto remoto

---

5. Verificare lo stato di sicurezza della rete.

- Utilizzare il Dashboard per visualizzare lo stato della rete. Per ulteriori informazioni relative al Dashboard, fare riferimento alla sezione Utilizzo del Dashboard

---

3.2 Gestione efficace delle patch

GFI LanGuard consente di gestire la distribuzione delle patch nella rete.

GFI LanGuard può supportare gli aggiornamenti delle patch per i seguenti prodotti:

- Sistemi operativi Windows®
- Applicazioni Microsoft®
- La maggioranza delle applicazioni di terze parti comunemente utilizzate (prodotti Adobe, runtime di Java e browser web)
- Sistemi operativi MAC

---

1. Utilizzare il Dashboard per visualizzare le patch mancanti:

- Visualizzazione Patch

---

2. Personalizzare il profilo di scansione delle patch:

- Configurazione delle patch

---

3. Riparare le vulnerabilità correlate alle patch mancanti:

- Distribuzione di patch di sicurezza e service pack
- Disinstallazione patch software e service pack

3.3 Utilizzo di GFI LanGuard per la tracciabilità asset

Le periferiche non gestite o dimenticate costituiscono un rischio di sicurezza. Per rilevare le periferiche non gestite o dimenticate, effettuare i seguenti passaggi:

1. Rilevare in automatico la presenza di nuovi dispositivi nella rete.

GFI LanGuard rileva in automatico la presenza di nuovi computer sulla rete:

- Enumera computer
- Individuazione di rete

2. Distribuire gli agenti nei nuovi computer rilevati.

- Distribuzione degli agenti
- Distribuzione manuale agenti
- Proprietà agente
- Impostazioni agenti

3. Utilizzare il Dashboard per visualizzare le vulnerabilità collegate ai nuovi computer.

- Panoramica
- Visualizzazione Computer
- Visualizzazione vulnerabilità
- Visualizzazione Software
- Visualizzazione Hardware
- Visualizzazione Informazioni di sistema

3.4 Analisi di rete e software aggiornata

L'analisi di rete consente di apprendere ulteriori dati su quanto accade nella propria rete, poiché rileva le configurazioni e le applicazioni che costituiscono un rischio di sicurezza sulla rete. Tali problemi possono essere identificati mediante le seguenti funzioni:

Visualizzazioni e strumenti GFI LanGuard

- Visualizzazione Software: per una visione dettagliata di tutte le applicazioni installate nella rete.
- Visualizzazione Hardware: per controllare l'inventario hardware della rete.
- Informazioni di sistema: per visualizzare i dati di sicurezza sensibili relativi ai sistemi presenti nella rete.
- Cronologia: per ottenere un elenco di modifiche di sicurezza sensibili che si sono verificate nella rete.
- Controllo software: per generare un rapporto completo relativo alle applicazioni installate nella rete.

Riparazione problemi

- Riparazione vulnerabilità
- Configurazione disinstallazione automatica applicazioni non autorizzate
- Distribuzione software personalizzato
- Disinstallazione delle applicazioni personalizzate
- Utilizzo del supporto remoto

3.5 Conformità a PCI DSS

Finalmente la piena conformità a PCI DSS, i severi standard di sicurezza stabiliti dalle principali aziende di carte di credito mondiali. Nel fornire una gestione completa delle vulnerabilità con funzionalità estesa di creazione rapporti, GFI LanGuard costituisce una soluzione essenziale per facilitare il programma di conformità PCI. Per ulteriori informazioni su come essere conformi a PCI DSS, utilizzare i seguenti collegamenti:

Modulo di registrazione per la conformità a PCI DSS e i prodotti GFI Software.

- http://go.gfi.com/?pageid=PCIDSS_Compliance_Whitepaper

Best practice

- Effettuare regolari valutazioni delle vulnerabilità. Fare riferimento alla sezione Scansione della rete.
- Riparare le vulnerabilità e distribuire le patch mancanti. Fare riferimento alla sezione Riparazione vulnerabilità.
- Generare rapporti e visualizzare lo stato dell'infrastruttura. Fare riferimento all'articolo Creazione di rapporti.
- Assicurarsi che il software antivirus e antispyware sia installato nei computer di destinazione. Per ottenere questo, eseguire una scansione sui computer di destinazione mediante il profilo di scansione **Controllo software**, accessibile dal gruppo Controllo rete e software. For more information, refer to Profili di scansione disponibili (page 65).
- Assicurarsi che il firewall personale sia installato nei computer di destinazione. For more information, refer to Scansioni manuali (page 67)..
- Assicurarsi che il software di crittografia sia installato nella rete. For more information, refer to Scansioni manuali (page 67)..

Altri prodotti GFI che possono facilitare il raggiungimento della conformità:

- GFI VIPRE: soluzione antivirus, antispyware e firewall personale
- GFI EventsManager: soluzione di gestione registro
- GFI EndPointSecurity: soluzione di blocco dispositivi

4 Gestione degli agenti

GFI LanGuard può essere configurato per la distribuzione automatica di agenti sui computer appena rilevati o per la distribuzione manuale di quelli selezionati. Gli agenti permettono controlli più rapidi e riducono notevolmente l'utilizzo della larghezza di banda della rete. Quando si utilizzano gli agenti, i controlli vengono eseguiti utilizzando la potenza delle risorse delle destinazioni di scansione. Una volta completato il controllo, i risultati vengono inviati a GFI LanGuard in un file XML.

Argomenti del presente capitolo:

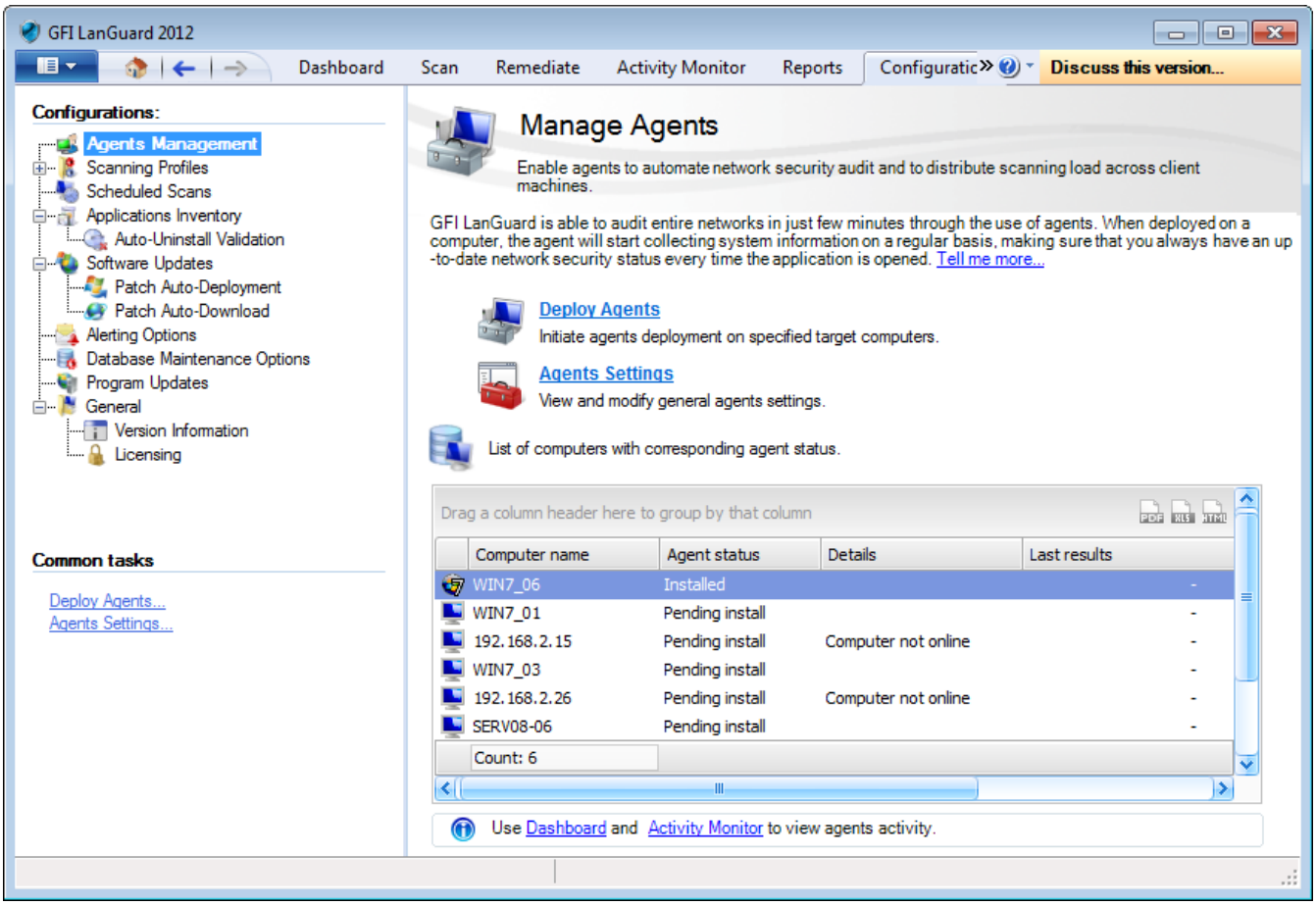
4.1 Distribuzione degli agenti 44
4.2 Distribuzione manuale agenti 46
4.3 Proprietà agente 49
4.4 Impostazioni agenti 53
4.5 Configurazione degli agenti relay 54
4.6 Gestione dei gruppi agente 62

4.1 Distribuzione degli agenti

Per distribuire gli agenti GFI LanGuard sui computer di rete:

1. Avviare GFI LanGuard.

2. **Dal menu Home** selezionare **Gestisci agenti**. In alternativa fare clic sulla scheda **Configurazione > Gestione agenti**.


GFI LanGuard 2012
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuratic
Discuss this version...
Configurations:
Agents Management
Scanning Profiles
Scheduled Scans
Applications Inventory
Auto-Uninstall Validation
Software Updates
Patch Auto-Deployment
Patch Auto-Download
Alerting Options
Database Maintenance Options
Program Updates
General
Version Information
Licensing
Common tasks
Deploy Agents...
Agents Settings...
Manage Agents
Enable agents to automate network security audit and to distribute scanning load across client machines.
GFI LanGuard is able to audit entire networks in just few minutes through the use of agents. When deployed on a computer, the agent will start collecting system information on a regular basis, making sure that you always have an up-to-date network security status every time the application is opened. Tell me more...
Deploy Agents
Initiate agents deployment on specified target computers.
Agents Settings
View and modify general agents settings.
List of computers with corresponding agent status.
Drag a column header here to group by that column
Computer name
Agent status
Details
Last results
WIN7_06 Installed
WIN7_01 Pending install
192.168.2.15 Pending install Computer not online
WIN7_03 Pending install
192.168.2.26 Pending install Computer not online
SERV08-06 Pending install
Count: 6
Use Dashboard and Activity Monitor to view agents activity.

Screenshot 13: Gestisci agenti

3. Per selezionare i computer di destinazione per la scansione, accedere alla sezione **Attività comuni** e fare clic su **Distribuisci agenti**, quindi fare clic su **Avanti**. Selezionare una delle opzioni descritte di seguito:

Table 12: Selezione destinazione

Opzione	Descrizione
Dominio locale	Distribuzione degli agenti su tutti i computer raggiungibili all'interno dello stesso gruppo di lavoro/dominio dove è installato GFI LanGuard. Nel passaggio **Definisci destinazione** non sono necessarie ulteriori operazioni di configurazione.
Personalizzato	Distribuzione degli agenti su computer specifici o gruppi di computer. Aggiungere nuove regole per la ricerca o l'indicazione dei computer di destinazione.

4. Se è stata selezionata l'opzione **Personalizzato**, fare clic su **Aggiungi nuova regola** e selezionare il **Tipo di regola** di seguito illustrato:

Table 13: Opzioni regole personalizzate

Tipo di regola	Descrizione
Nome computer è	Immettere manualmente un nome per il computer o importare i nomi da un file di testo salvato (.txt). Fare clic su **Seleziona** e scegliere manualmente i computer dall'elenco, oppure fare clic su **Importa** e specificare il percorso del file di testo.
Nome dominio è	Selezionare i domini dall'elenco di domini raggiungibili.

Tipo di regola	Descrizione
Unità organizzativa è	Selezionare i computer da una o più unità organizzative raggiungibili. Utilizzare le seguenti opzioni: » **Recupera**: digitare il nome utente e la password per recuperare l'elenco » **Aggiorna**: aggiornare l'elenco dei domini e delle unità organizzative » **Aggiungi**: aggiunge manualmente un'unità organizzativa.

Ripetere il passaggio 4 per ciascuna regola. Al termine, fare clic su **OK**.

5. Dalla finestra di dialogo **Distribuisci agenti**, fare clic su **Avanti**.

6. (Facoltativo) Per specificare credenziali alternative, selezionare la casella di controllo **Autenticazione tramite**.

7. (Facoltativo) Fare clic su **Impostazioni avanzate** e configurare le impostazioni delle schede seguenti:

Table 14: Distribuisci agenti: Impostazioni avanzate

Scheda	Descrizione
Generale	Configurare la pianificazione in base alla quale GFI LanGuard esegue la ricerca automatica di nuovi computer nel perimetro di rete dove sono abilitati gli agenti.
Pianificazione controllo	Configura la frequenza con cui l'agente controlla il computer host (dove è installato l'agente). Selezionare il criterio di ricorrenza e l'orario in cui inizierà il controllo.
Riparazione automatica	Configurare GFI LanGuard per l'installazione e il download automatico di patch e service pack mancanti. Disinstalla le applicazioni non autorizzate nei computer scansionati. For more information, refer to Riparazione automatica (page 120).

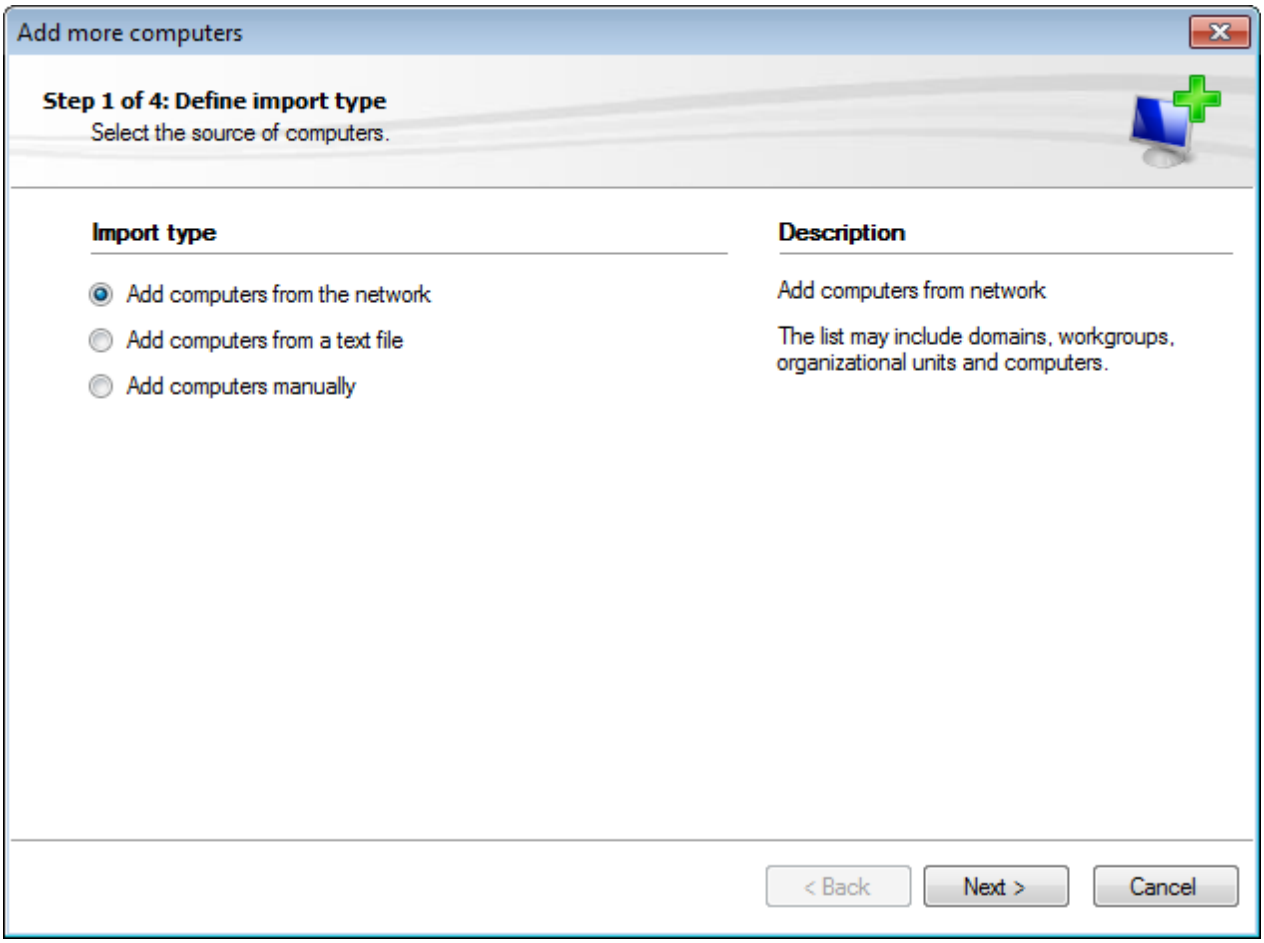
8. Per completare la distribuzione dell'agente, fare clic su **Avanti** e **Fine**.

4.2 Distribuzione manuale agenti

Per distribuire manualmente gli agenti:

1. Avviare GFI LanGuard e selezionare **Dashboard**.

2. Da **Attività comuni** selezionare **Aggiungi altri computer**.


Add more computers
Step 1 of 4: Define import type
Select the source of computers.
Import type
Add computers from the network
Add computers from a text file
Add computers manually
Description
Add computers from network
The list may include domains, workgroups, organizational units and computers.
< Back
Next >
Cancel

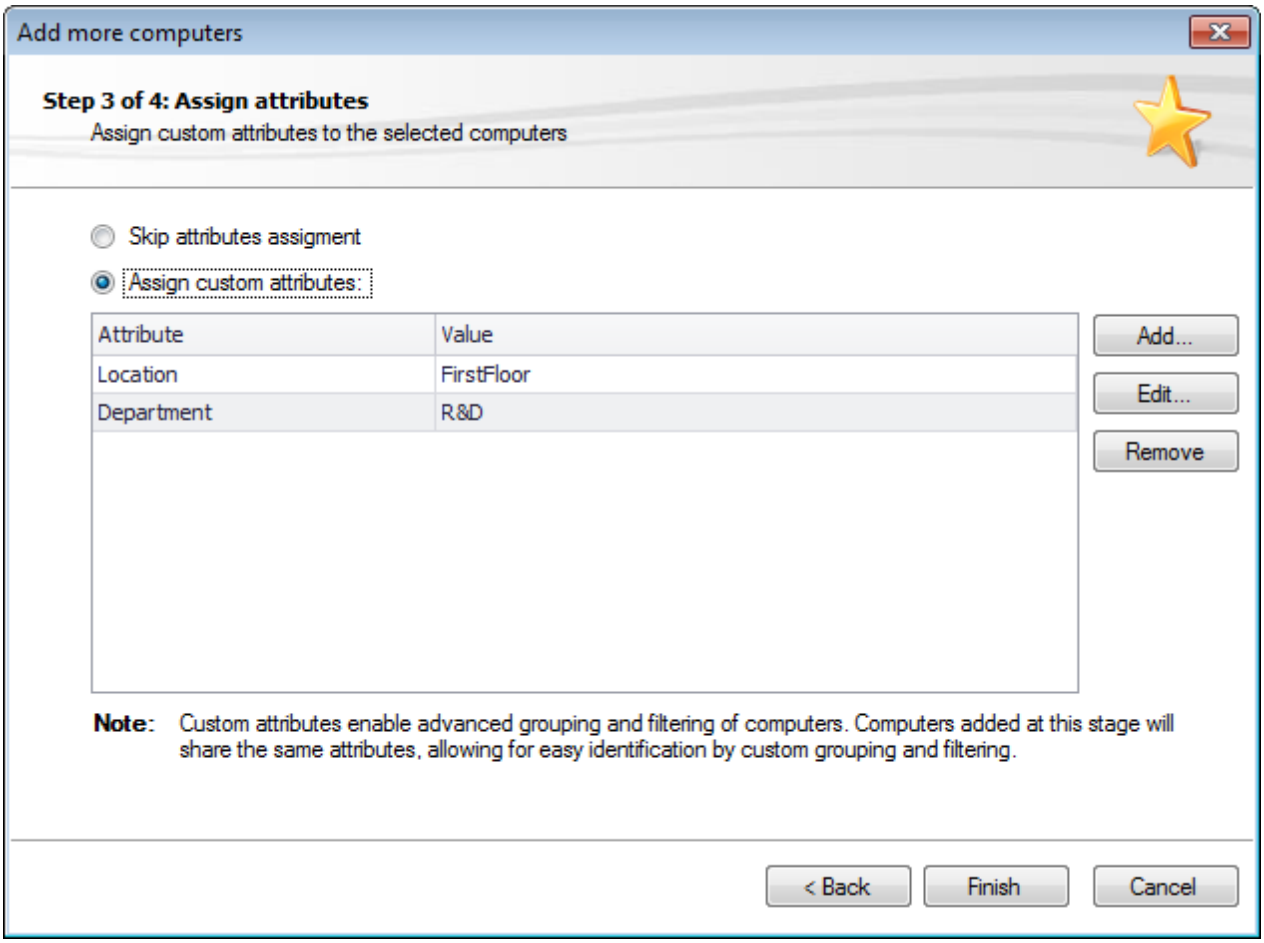
Screenshot 14: Aggiungi altri computer - Selezione del tipo per l'importazione

3. Dalla procedura guidata Aggiungi altri computer selezionare una delle seguenti opzioni:

Table 15: Procedura guidata Aggiungi altri computer

Opzione	Descrizione
Aggiungi computer dalla rete	Selezionare i domini, le unità organizzative e i computer dall'elenco. Per aggiungere un nuovo dominio all'elenco di computer, utilizzare l'opzione **Aggiungi dominio**.
Aggiungi computer da un file di testo	Importa l'elenco computer da un file di testo. Fare clic su **Sfoglia**, quindi individuare il file di testo contenente l'elenco dei computer.
Aggiungi computer manualmente	Crea manualmente un elenco di computer. Per aggiungere e rimuovere computer dall'elenco, fare clic sui pulsanti **Aggiungi** e **Rimuovi**. Per importare ed esportare l'elenco da/a un file di testo, utilizzare i pulsanti **Importa** ed **Esporta**.

Fare clic su **Avanti**.



Screenshot 15: Aggiungi altri computer - Assegnazione di attributi ai nuovi computer

4. Per facilitare il raggruppamento e il filtraggio, è possibile assegnare attributi personalizzati a computer specifici. Dalla procedura guidata **Assegnazione attributi**, configurare quanto segue:

Table 16: Impostazioni attributi

Opzione	Descrizione
Ignora assegnazione attributi	Non sono stati aggiunti attributi all'elenco computer.
Assegna attributi personalizzati	Assegna gli attributi a un elenco di computer. Fare clic sul pulsante **Aggiungi**, quindi specificare il nuovo nome dell'attributo e il relativo valore. **Nota** Quando si esegue l'importazione di un elenco di computer da un file di testo, GFI LanGuard assegna automaticamente il nome del file come attributo (File) all'elenco importato.

5. Fare clic su **Fine**.

Nota

Se i computer selezionati dispongono di credenziali di accesso diverse rispetto al computer GFI LanGuard, GFI LanGuard apre una finestra di dialogo che consente di specificare credenziali valide.

6. Una volta aggiunti i computer all'elenco, fare clic su **Chiudi**.

7. Dalla struttura computer, fare clic con il pulsante destro del mouse sui computer aggiunti e selezionare quelli in cui distribuire l'agente. Da **Stato agente** fare clic su **Distribuisci agente**.

8. Configurare le proprietà dell'agente. For more information, refer to Proprietà agente (page 49).

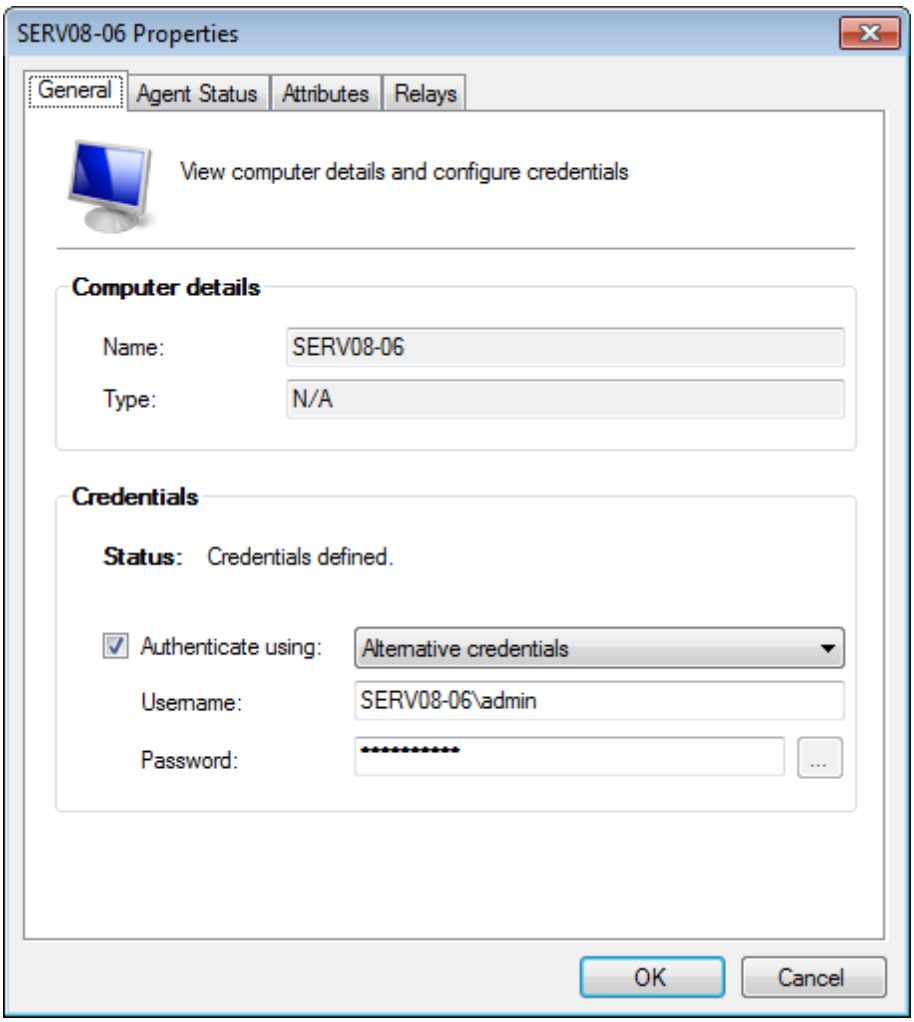
4.3 Proprietà agente

Per modificare le proprietà dell'agente:

1. Fare clic sulla scheda **Configurazione>Gestione agenti**.

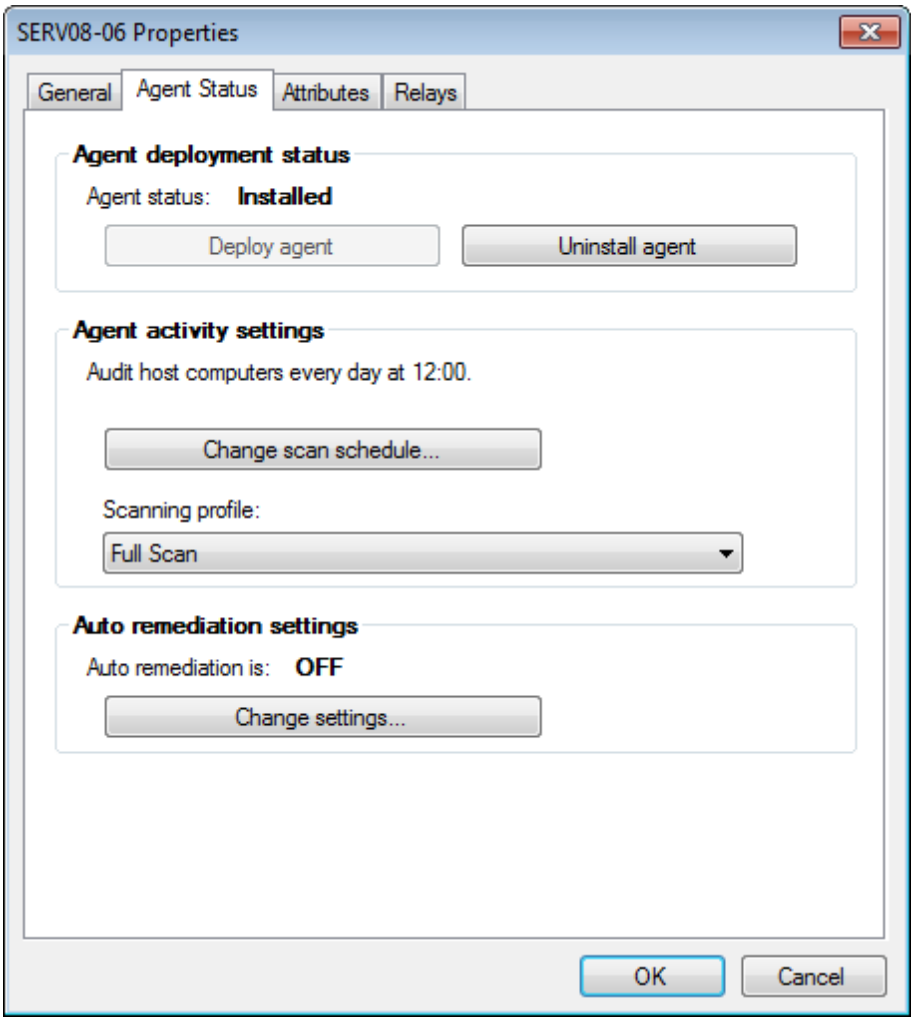
2. Dal riquadro a destra, fare clic con il pulsante destro del mouse su un agente, quindi selezionare **Proprietà**.

> **Nota**
>
> La finestra di dialogo **Proprietà** è accessibile dalla struttura computer all'interno del **Dashboard**. Fare clic con il pulsante destro del mouse su un computer o gruppo e selezionare **Proprietà**.



Screenshot 16: Proprietà agente - scheda Generale

3. (Facoltativo) Dalla scheda **Generale** specificare il nome, il tipo e il metodo di autenticazione per l'agente selezionato.



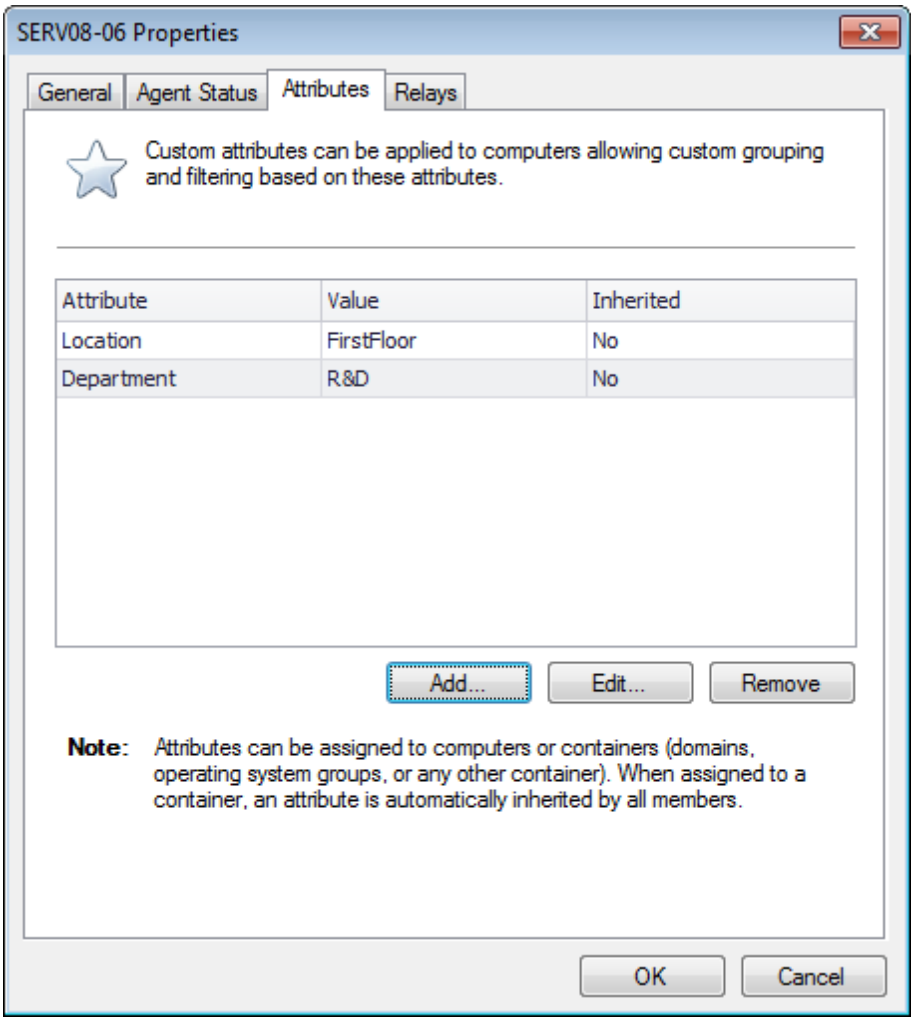
Screenshot 17: Proprietà agente - scheda Stato agente

4. Dalla scheda **Stato agente**, abilitare/disabilitare la distribuzione dell'agente selezionando **Distribuisci agente** o **Impedisci installazione agente**.

5. Per configurare la pianificazione di scansione dell'agente fare clic su **Modifica pianificazione di scansione...** per configurare la pianificazione di scansione dell'agente selezionato.

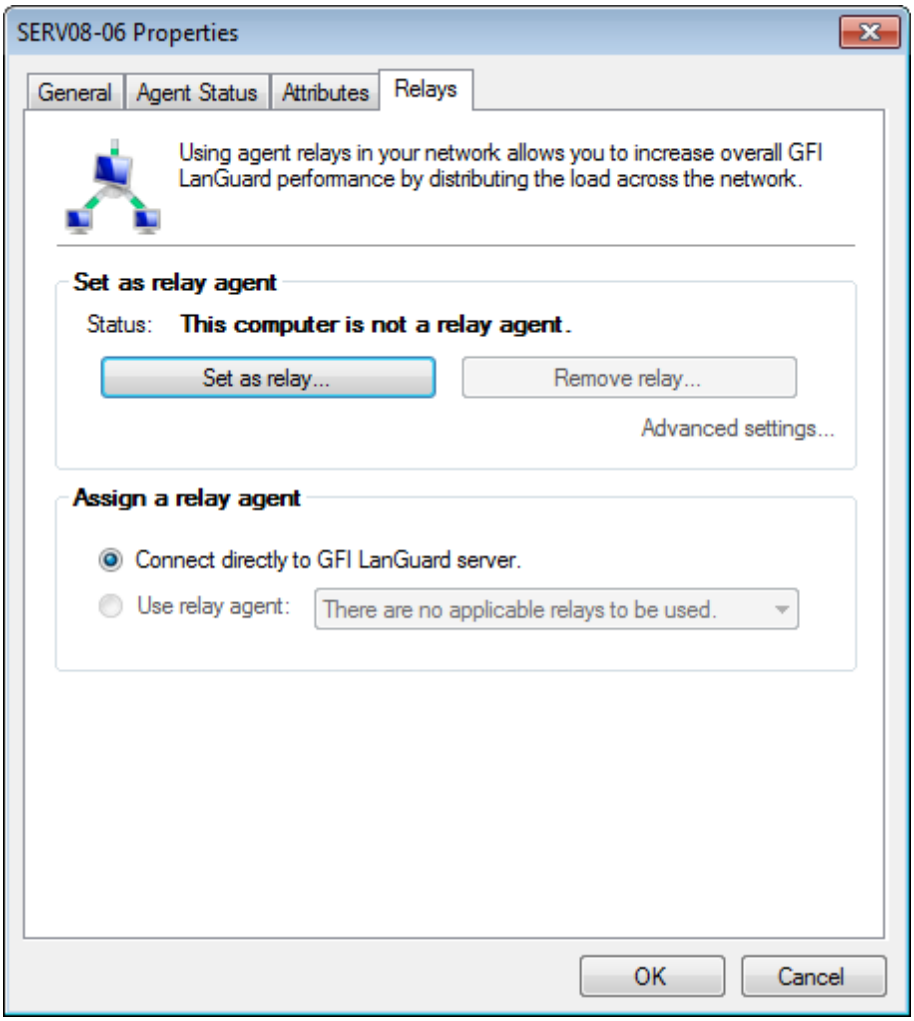
6. Da **Profilo di scansione** selezionare il profilo di scansione attivo.

7. Per abilitare/disabilitare la riparazione automatica dell'agente, fare clic su **Cambia impostazioni...** da **Impostazioni di riparazione automatica**. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).



Screenshot 18: Proprietà agente - scheda Attributi

8. Selezionare la scheda **Attributi** per gestire gli attributi assegnati al computer selezionato. Per gestire gli attributi, utilizzare i pulsanti **Aggiungi**, **Modifica** e **Rimuovi**.


SERV08-06 Properties
General
Agent Status
Attributes
Relays
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.
Set as relay agent
Status: This computer is not a relay agent.
Set as relay...
Remove relay...
Advanced settings...
Assign a relay agent
Connect directly to GFI LanGuard server.
Use relay agent:
There are no applicable relays to be used.
OK
Cancel

Screenshot 19: Proprietà agente - scheda Relay

9. Per configurare i relay degli agenti, fare clic sulla scheda **Relay**. I relay consentono ai computer diversi da quello che ospita GFI LanGuard di agire come server di GFI LanGuard. Ciò consente di bilanciare il carico del traffico diretto a quel computer e di ottimizzare le prestazioni di scansione della rete.

10. Configurare le opzioni descritte di seguito:

Table 17: Opzioni relay agente

Opzione	Descrizione
Imposta come relay	Imposta il computer selezionato come agente relay. Il computer selezionato invierà gli aggiornamenti del prodotto e le patch agli altri agenti per ridurre il carico del computer dove è eseguito GFI LanGuard. Fare clic su **Imposta come relay...** e seguire la procedura guidata di configurazione.
Rimuovi relay	Rimuove il ruolo dell'agente relay dal computer selezionato. Fare clic su **Rimuovi relay...** e seguire la procedura guidata di configurazione.
Connetti direttamente al server GFI LanGuard	Il computer selezionato scaricherà gli aggiornamenti del prodotto e le patch dal server di GFI LanGuard.
Usa agente relay	Il computer selezionato utilizzerà un agente relay per scaricare gli aggiornamenti del prodotto e le patch. Nell'elenco a discesa, selezionare l'agente relay da utilizzare.

11. (Facoltativo) Fare clic su **Impostazioni avanzate** e configurare le seguenti opzioni:

Table 18: Impostazioni avanzate agente relay

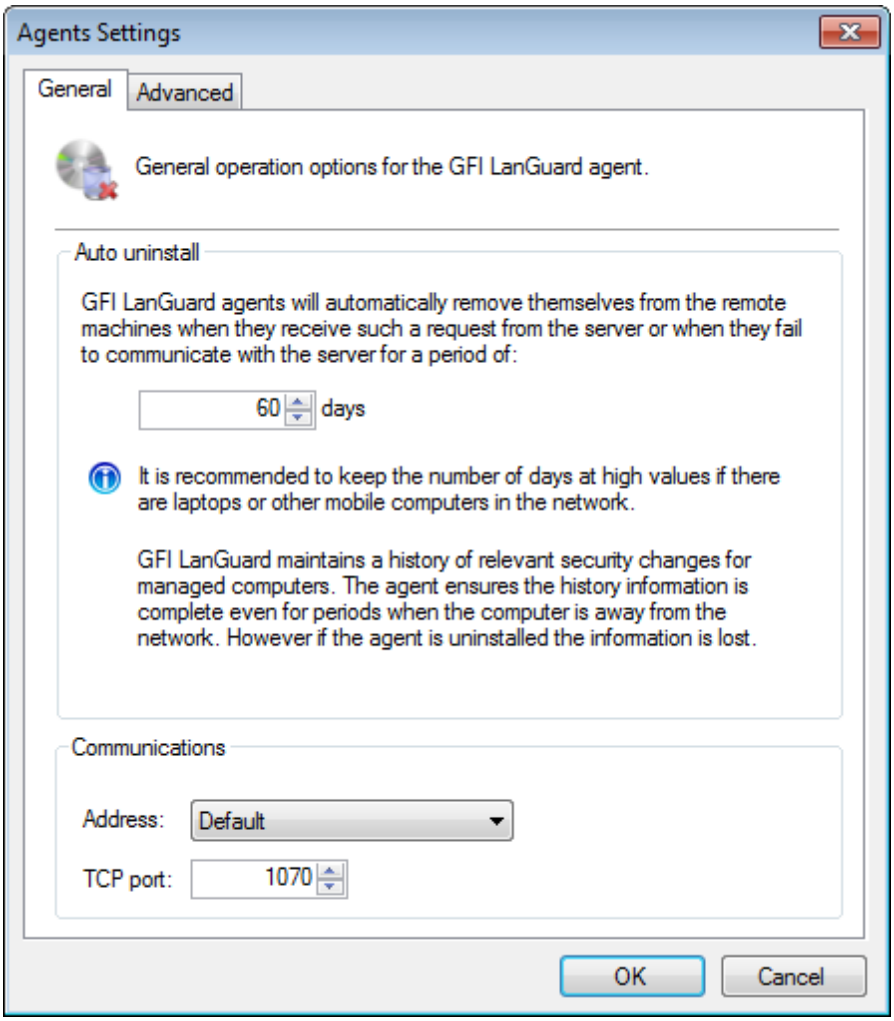
Opzione	Descrizione
Directory di memorizzazione nella cache	Tutte le patch e gli aggiornamenti vengono memorizzati in questa posizione prima di essere installati nel computer client.
Porta di comunicazione	La porta utilizzata dall'agente relay per elaborare le richieste.
Indirizzo del server	L'indirizzo utilizzato dai computer client per la connessione all'agente relay (per impostazione predefinita viene utilizzato il nome host del DNS).

12. Fare due volte clic su **OK**.

4.4 Impostazioni agenti

Per configurare le impostazioni aggiuntive degli agenti:

1. Dalla scheda **Configurazione**, selezionare **Gestione agenti**.
2. Fare clic su **Impostazioni agenti**.


Agents Settings
General
Advanced
General operation options for the GFI LanGuard agent.
Auto uninstall
GFI LanGuard agents will automatically remove themselves from the remote machines when they receive such a request from the server or when they fail to communicate with the server for a period of:
60
days
It is recommended to keep the number of days at high values if there are laptops or other mobile computers in the network.
GFI LanGuard maintains a history of relevant security changes for managed computers. The agent ensures the history information is complete even for periods when the computer is away from the network. However if the agent is uninstalled the information is lost.
Communications
Address:
Default
TCP port:
1070
OK
Cancel

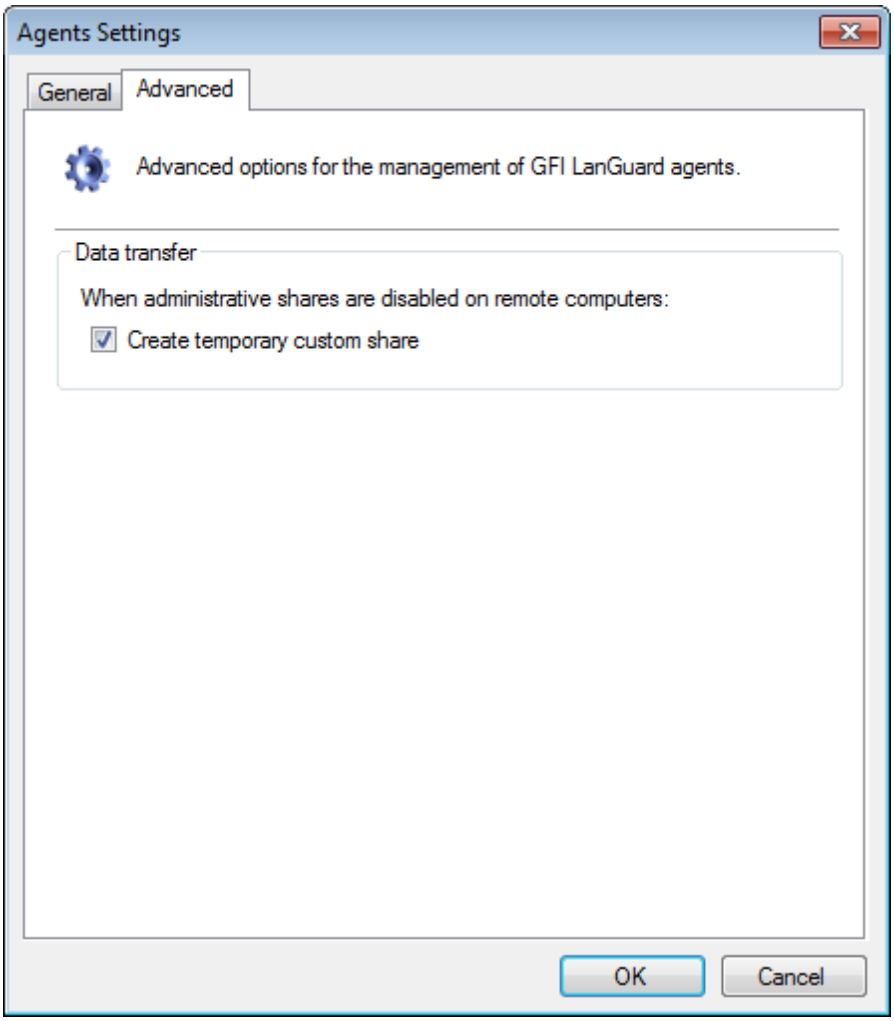
Screenshot 20: Impostazioni agente - scheda Generale

3. Configurare le opzioni descritte di seguito:

Table 19: Impostazioni agenti

Opzione	Descrizione
Disinstallazione automatica	Impostare il numero di giorni trascorsi i quali gli agenti di GFI LanGuard si disinstallano in automatico qualora il computer host non risponda per un determinato periodo di giorni.

Opzione	Descrizione
Gli agenti creano rapporti tramite	Configurare la porta e l'indirizzo IP utilizzati dagli agenti per comunicare e segnalare lo stato a GFI LanGuard. Quando il computer GFI LanGuard dispone di indirizzi IP multipli ed è selezionata l'impostazione Predefinito, GFI LanGuard seleziona automaticamente l'indirizzo IP da utilizzare.



Screenshot 21: Impostazioni agente - scheda Avanzate

4. (Facoltativo) Fare clic sulla scheda **Avanzate** e selezionare **Crea condivisione personalizzata temporanea**. Quando questa opzione è abilitata e nei computer degli agenti sono disabilitate le condivisioni amministrative, GFI LanGuard crea una cartella condivisa temporanea per il trasferimento delle informazioni.

5. Fare clic su **OK** per salvare e chiudere la finestra di dialogo.

AVVISO

Affinché gli agenti GFI LanGuard possano inviare dati a GFI LanGuard, è necessario abilitare sul firewall di Windows la comunicazione sulla porta **1070**.

4.5 Configurazione degli agenti relay

Nelle reti di dimensioni maggiori è probabile che le prestazioni siano compromesse a causa del numero di destinazioni di scansione e del volume di dati trasferiti al componente server GFI LanGuard. Ne risultano rallentamenti nella velocità di scansione e nel recupero dei dati di scansione.

Per evitare problemi di prestazioni e applicare tecniche di bilanciamento del carico, GFI LanGuard consente di configurare gli agenti affinché agiscano da relay del server. Gli agenti configurati come agenti relay scaricano le patch e le definizioni direttamente dal server GFI LanGuard e le inoltrano ai computer client (che possono essere computer basati su agenti oppure senza agenti). I vantaggi principali nell'utilizzo degli agenti relay includono:

- Consumo ridotto della larghezza di banda della rete nelle reti locali o distribuite geograficamente. Se l'agente relay è configurato su ciascun lato, una patch viene scaricata una sola volta e distribuita ai computer client
- Carico delle prestazioni ridotto dal componente server di GFI LanGuard e distribuito negli agenti relay
- L'utilizzo di più agenti relay aumenta il numero di dispositivi che possono essere protetti contemporaneamente.

Gli agenti relay si comportano alla stessa maniera di GFI LanGuard e sono in grado di gestire le operazioni di controllo sicurezza e riparazione in altre destinazioni collegate al relay.

Per ulteriori informazioni, fare riferimento alle seguenti sezioni:

- Configurazione di un agente come relay
- Configurazione delle opzioni avanzate di un agente relay
- Connessione di computer a un agente relay

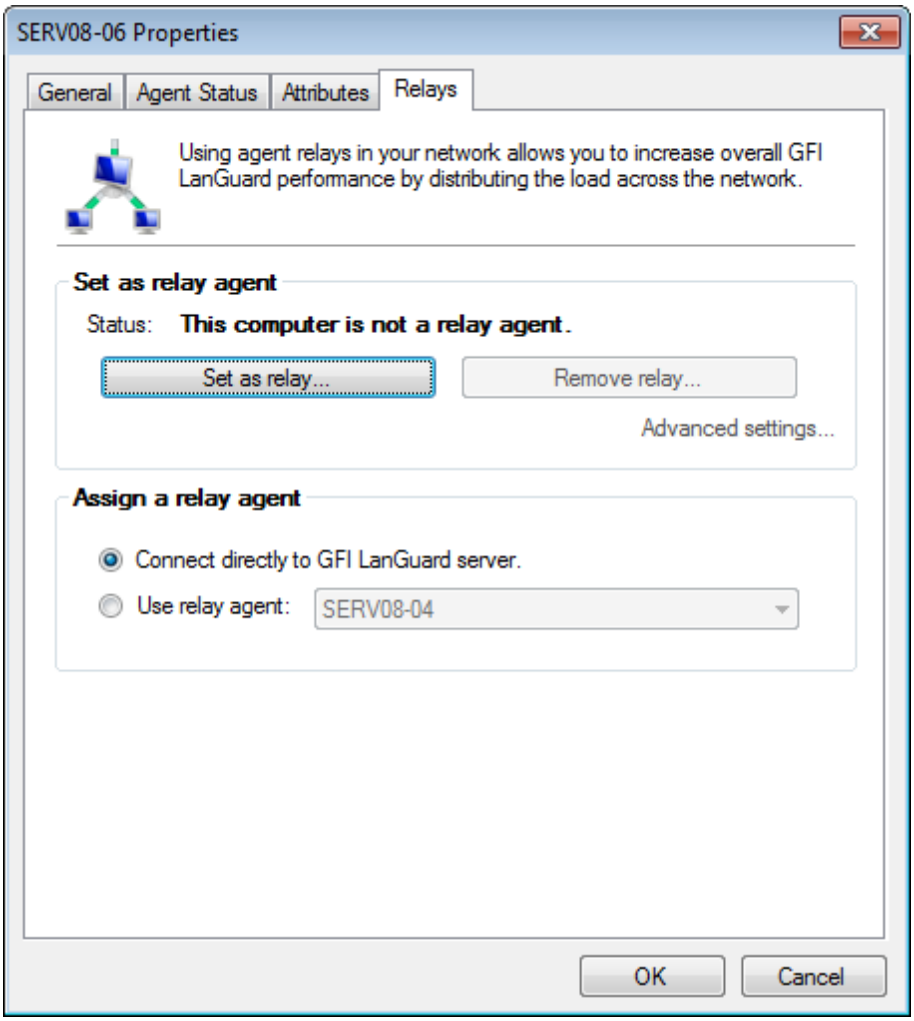
4.5.1 Configurazione di un agente come relay

Per configurare un agente con funzione di agente relay:

> **Nota**
>
> Il computer in cui è installato GFI LanGuard non può essere configurato come agente relay. La scheda **Relay** della finestra di dialogo **Proprietà** dell'agente risulta mancante per l'host GFI LanGuard.

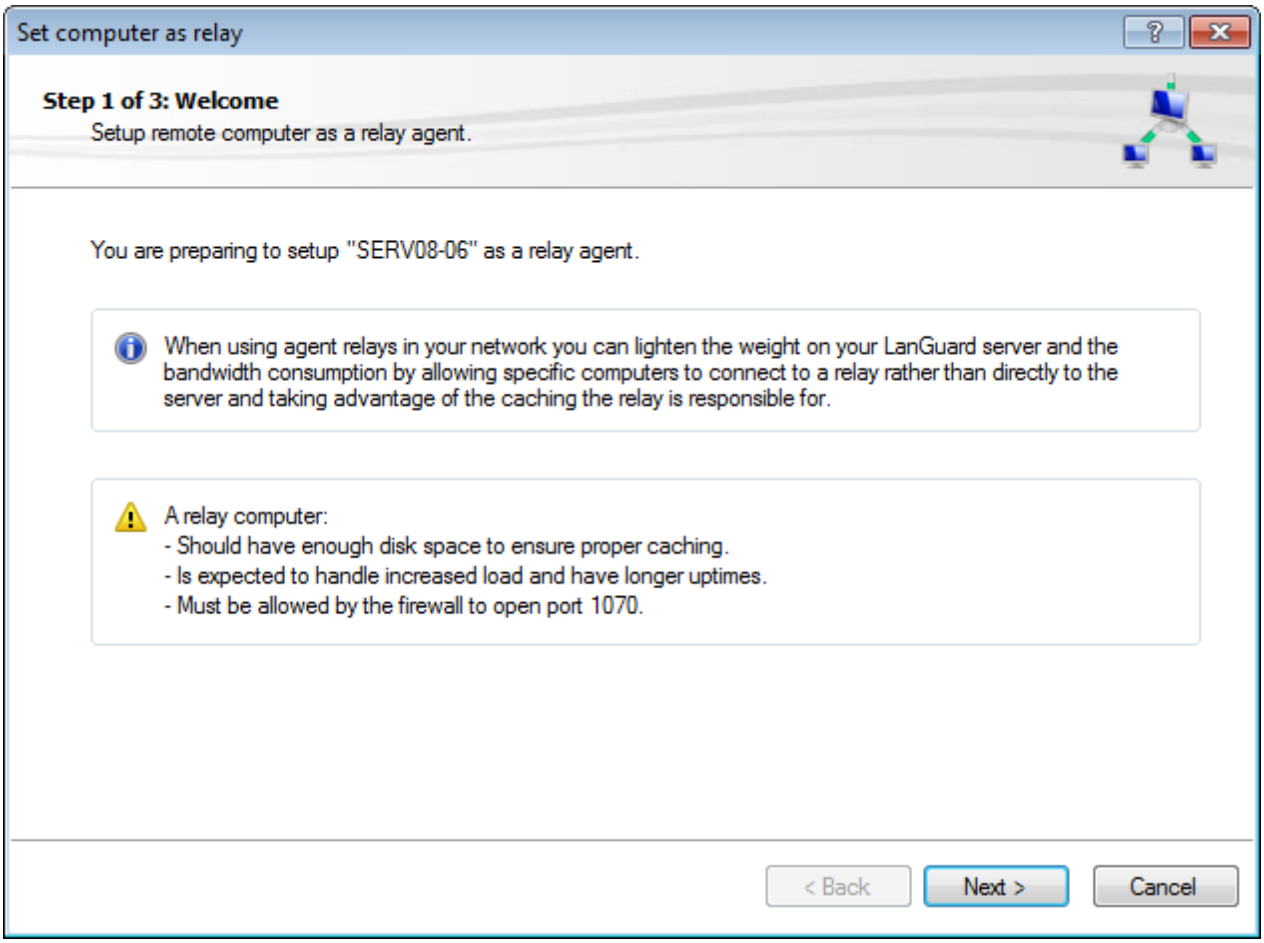
1. Aprire GFI LanGuard.
2. Fare sulla scheda **Configurazione > Gestione agenti**.
3. Fare clic con il pulsante destro del mouse sull'agente che si desidera configurare e selezionare **Proprietà**. Verrà aperta la finestra di dialogo **Proprietà** dell'agente.

> **Nota**
>
> In alternativa, dalla struttura computer fare clic con il pulsante destro del mouse sul computer/gruppo, quindi selezionare **Proprietà**.



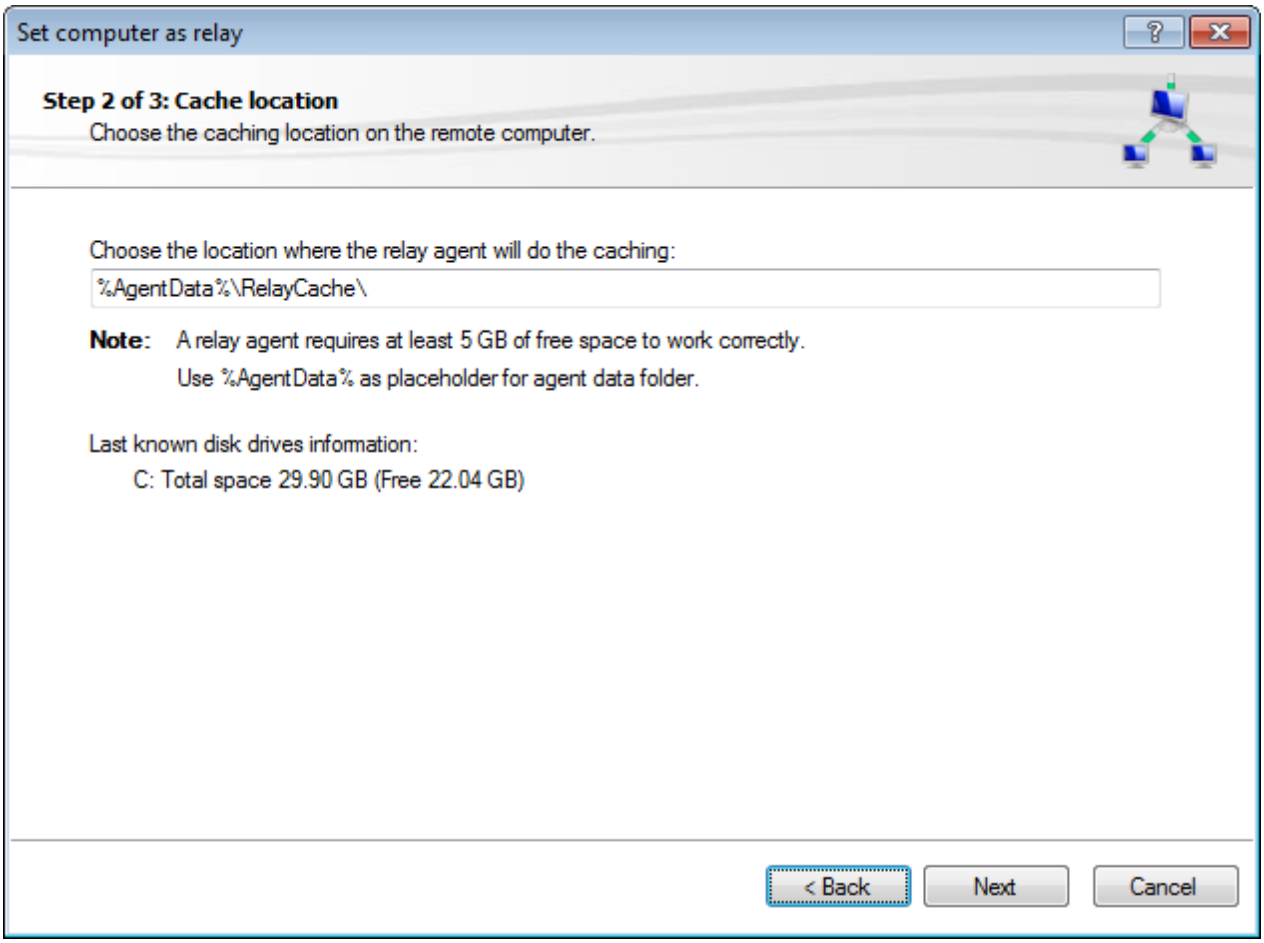
Screenshot 22: Finestra di dialogo Proprietà agente

4. Dalla scheda **Relay** fare clic su **Imposta come relay...**


Set computer as relay
Step 1 of 3: Welcome
Setup remote computer as a relay agent.
You are preparing to setup "SERV08-06" as a relay agent.
When using agent relays in your network you can lighten the weight on your LanGuard server and the bandwidth consumption by allowing specific computers to connect to a relay rather than directly to the server and taking advantage of the caching the relay is responsible for.
A relay computer:
- Should have enough disk space to ensure proper caching.
- Is expected to handle increased load and have longer uptimes.
- Must be allowed by the firewall to open port 1070.
< Back
Next >
Cancel

Screenshot 23: Imposta computer come procedura guidata relay

5. Leggere attentamente le note sui requisiti delle risorse per il computer in esecuzione come agente relay. Fare clic su **Avanti**.

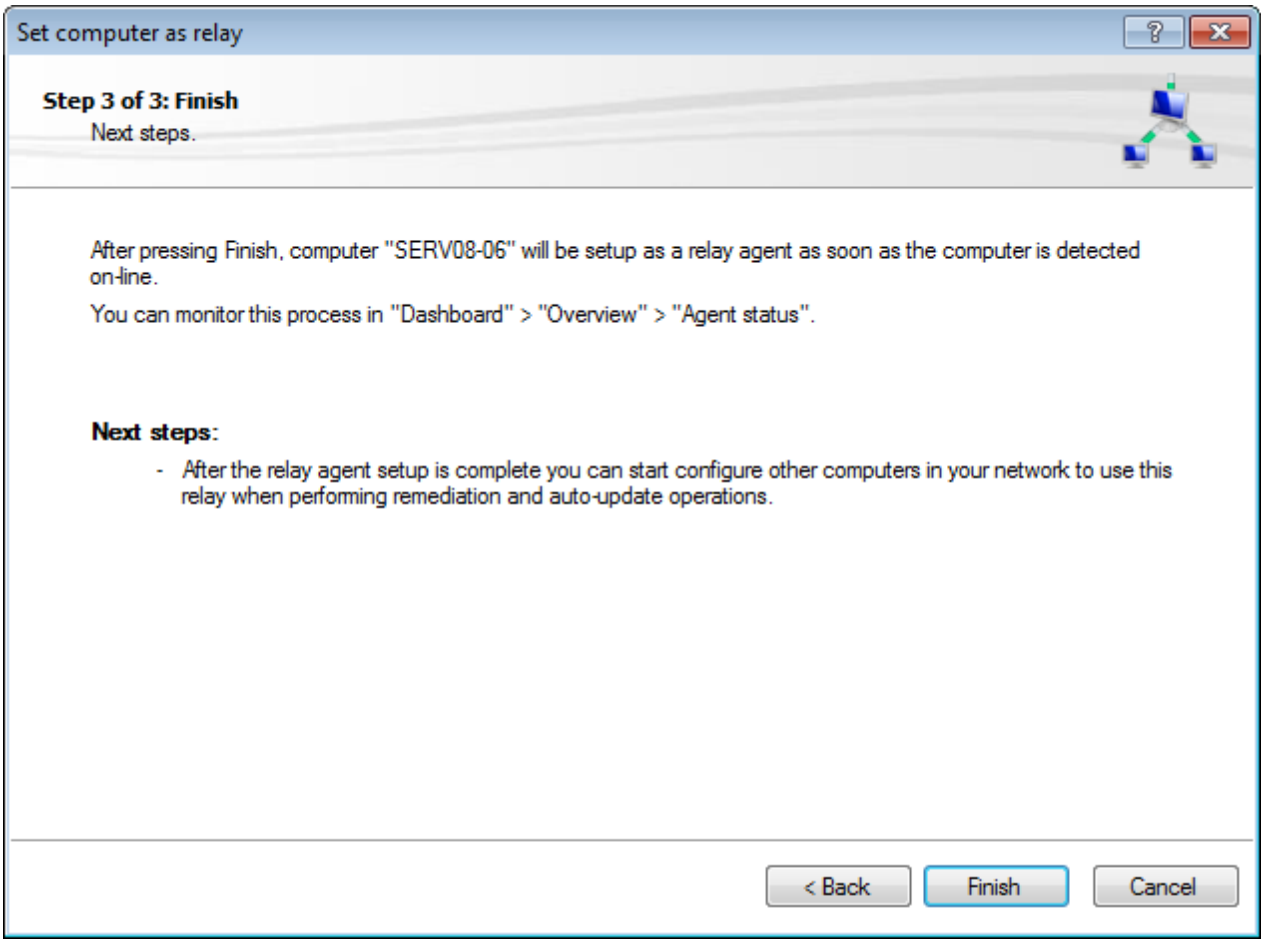

Set computer as relay
Step 2 of 3: Cache location
Choose the caching location on the remote computer.
Choose the location where the relay agent will do the caching:
%AgentData%\RelayCache\
Note: A relay agent requires at least 5 GB of free space to work correctly.
Use %AgentData% as placeholder for agent data folder.
Last known disk drives information:
C: Total space 29.90 GB (Free 22.04 GB)
< Back
Next
Cancel

Screenshot 24: Scegliere la directory di memorizzazione nella cache per il nuovo agente relay

6. Scegliere la posizione di memorizzazione nella cache per l'agente relay. La directory di memorizzazione nella cache viene utilizzata dal relay per archiviare le informazioni sul controllo e sulla riparazione quando si esegue il controllo dei computer remoti. Per impostazione predefinita, la cartella **RelayCache** viene creata in `C:\ProgramData\GFI\LanGuard 11\RelayCache`. Fare clic su **Avanti**.

Nota

Utilizzare il segnaposto **%AgentData%** per un riferimento rapido alla cartella dei dati dell'agente.


Set computer as relay
Step 3 of 3: Finish
Next steps.
After pressing Finish, computer "SERV08-06" will be setup as a relay agent as soon as the computer is detected on-line.
You can monitor this process in "Dashboard" > "Overview" > "Agent status".
Next steps:
- After the relay agent setup is complete you can start configure other computers in your network to use this relay when performing remediation and auto-update operations.
< Back
Finish
Cancel

Screenshot 25: Passaggio riepilogativo delle impostazioni

7. Fare clic su **Fine**.

> **Nota**
>
> Dopo aver selezionato **Fine**, l'agente selezionato sarà configurato come agente relay. È possibile monitorare il processo in **Dashboard > Panoramica > Stato agente**.

4.5.2 Configurazione delle opzioni avanzate di un agente relay

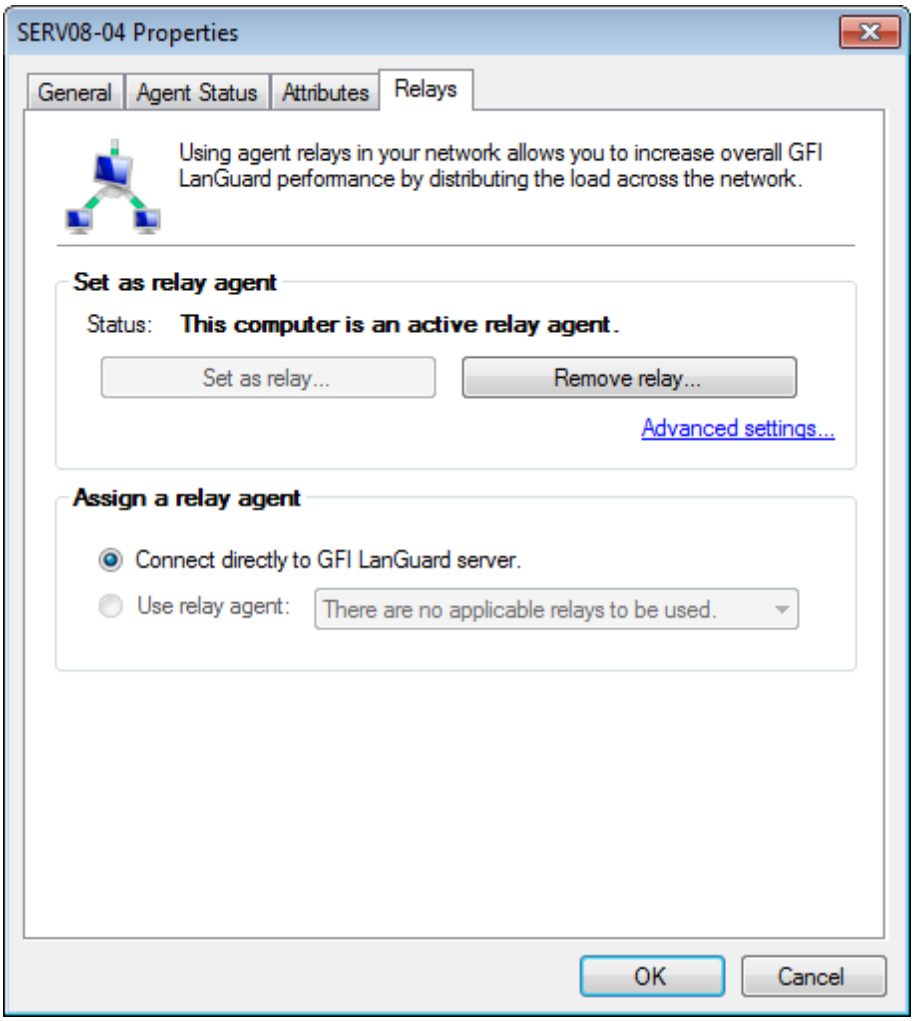
Per configurare le opzioni avanzate di un agente relay:

1. Aprire GFI LanGuard.

2. Fare sulla scheda **Configurazione > Gestione agenti**.

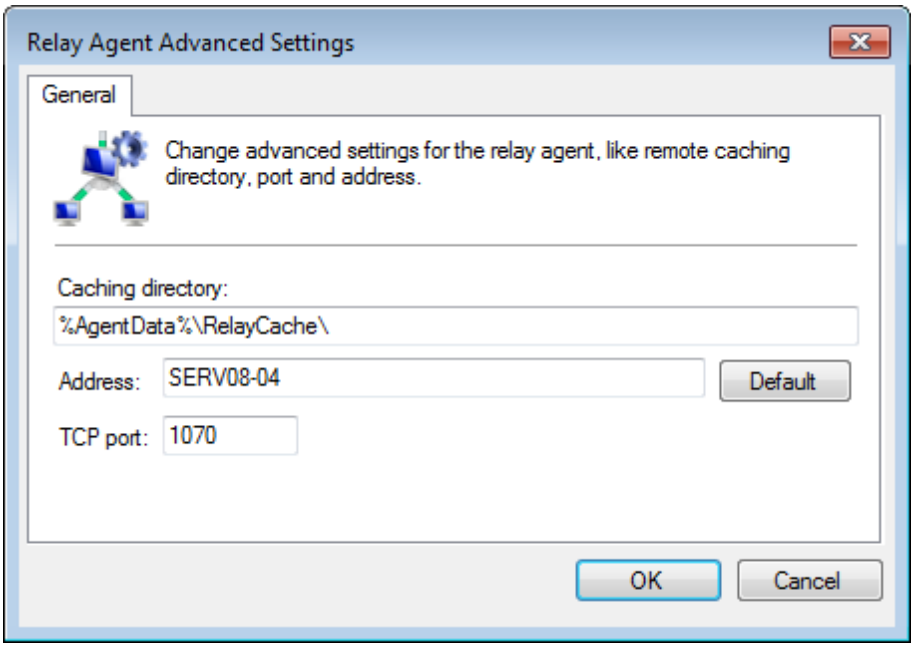
3. Fare clic con il pulsante destro del mouse sull'agente che si desidera configurare e selezionare **Proprietà**. Verrà aperta la finestra di dialogo **Proprietà** dell'agente.

> **Nota**
>
> In alternativa, dalla struttura computer fare clic con il pulsante destro del mouse sul computer/gruppo, quindi selezionare **Proprietà**.


SERV08-04 Properties
General
Agent Status
Attributes
Relays
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.
Set as relay agent
Status: This computer is an active relay agent.
Set as relay...
Remove relay...
Advanced settings...
Assign a relay agent
Connect directly to GFI LanGuard server.
Use relay agent:
There are no applicable relays to be used.
OK
Cancel

Screenshot 26: Proprietà agente relay - Impostazioni avanzate

4. Fare clic sulla scheda **Relay > Impostazioni avanzate...**



Screenshot 27: Finestra di dialogo delle impostazioni avanzate dell'agente relay

5. Dalla finestra di dialogo **Impostazioni avanzate agente di relay** configurare le opzioni descritte di seguito:

Table 20: Agente relay - Opzioni avanzate

Opzione	Descrizione
Directory di memorizzazione nella cache	La posizione in cui l'agente relay memorizza nella cache le informazioni durante il controllo dei computer remoti.
Indirizzo	Visualizza il nome computer che esegue l'agente relay. Fare clic su **Impostazione predefinita** per ripristinare il campo sul valore originale.
Porta TCP	La porta di comunicazione utilizzata dall'agente relay per comunicare con il server GFI LanGuard. La porta 1070 viene assegnata per impostazione predefinita e viene automaticamente modificata se GFI LanGuard rileva che la porta 1070 viene utilizzata da un'altra applicazione.

6. Fare clic su **OK**.

4.5.3 Connessione di computer a un relay

Per connettere un computer a un relay:

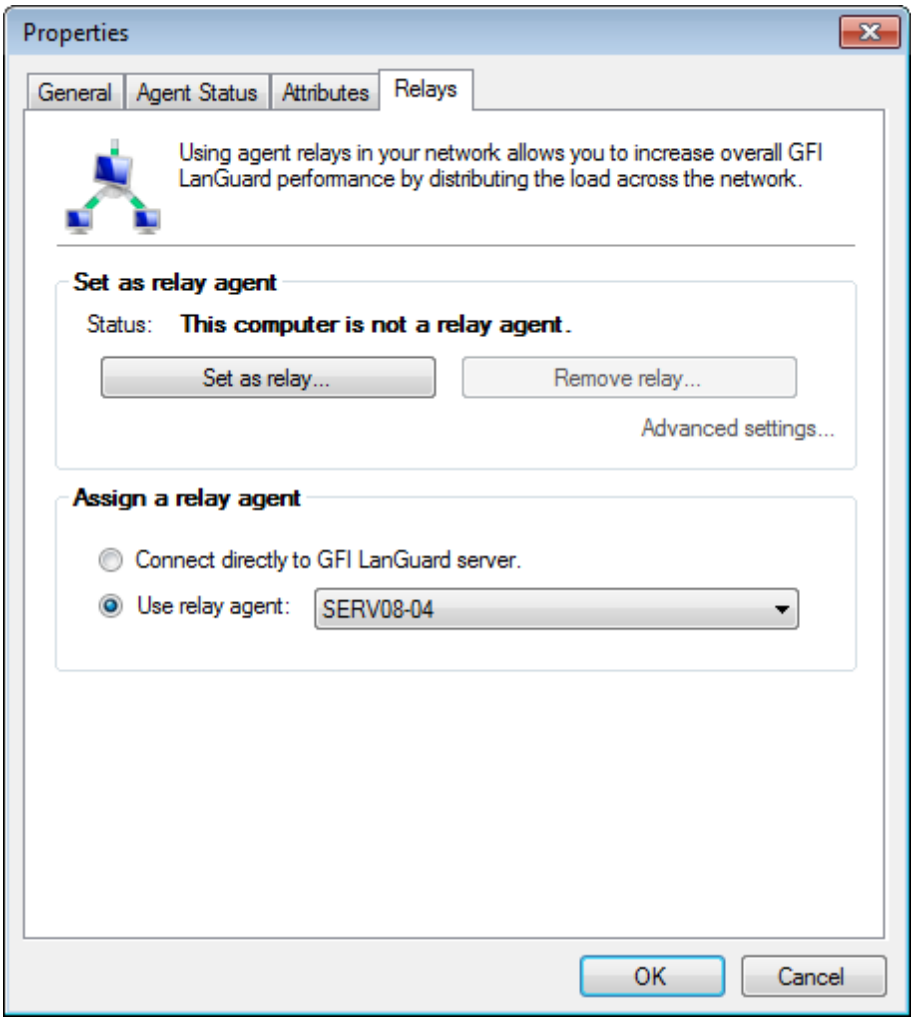
1. Aprire GFI LanGuard.

2. Fare sulla scheda **Configurazione > Gestione agenti**.

3. Fare clic con il pulsante destro del mouse sull'agente che si desidera configurare e selezionare **Proprietà**. Verrà aperta la finestra di dialogo **Proprietà** dell'agente.

> **Nota**
>
> In alternativa, dalla struttura computer fare clic con il pulsante destro del mouse sul computer/gruppo, quindi selezionare **Proprietà**.

4. Fare clic sulla scheda **Relay**.



Screenshot 28: Connessione a un agente relay

5. Dalla sezione **Assegna un agente di relay** selezionare **Usa agente relay** e scegliere il relay dal menu a discesa.

6. Fare clic su **OK**.

4.6 Gestione dei gruppi agente

La struttura computer consente di configurare le proprietà degli agenti di gruppi di computer. Per configurare le proprietà di gruppi di computer:

1. Dalla struttura computer fare clic con il pulsante destro del mouse su un gruppo di computer, quindi fare clic su **Proprietà**.

2. (Facoltativo) Dalla scheda **Generale** specificare il nome, il tipo e il metodo di autenticazione per il gruppo selezionato.

3. Selezionare la scheda **Stato agente** e configurare le seguenti opzioni:

Table 21: Stato gruppo agente

Opzione	Descrizione
Abilita distribuzione automatica agenti	Distribuisce automaticamente gli agenti sui nuovi computer rilevati.
Rimuovi tutti gli agenti	Rimuove tutti gli agenti installati da questo gruppo.

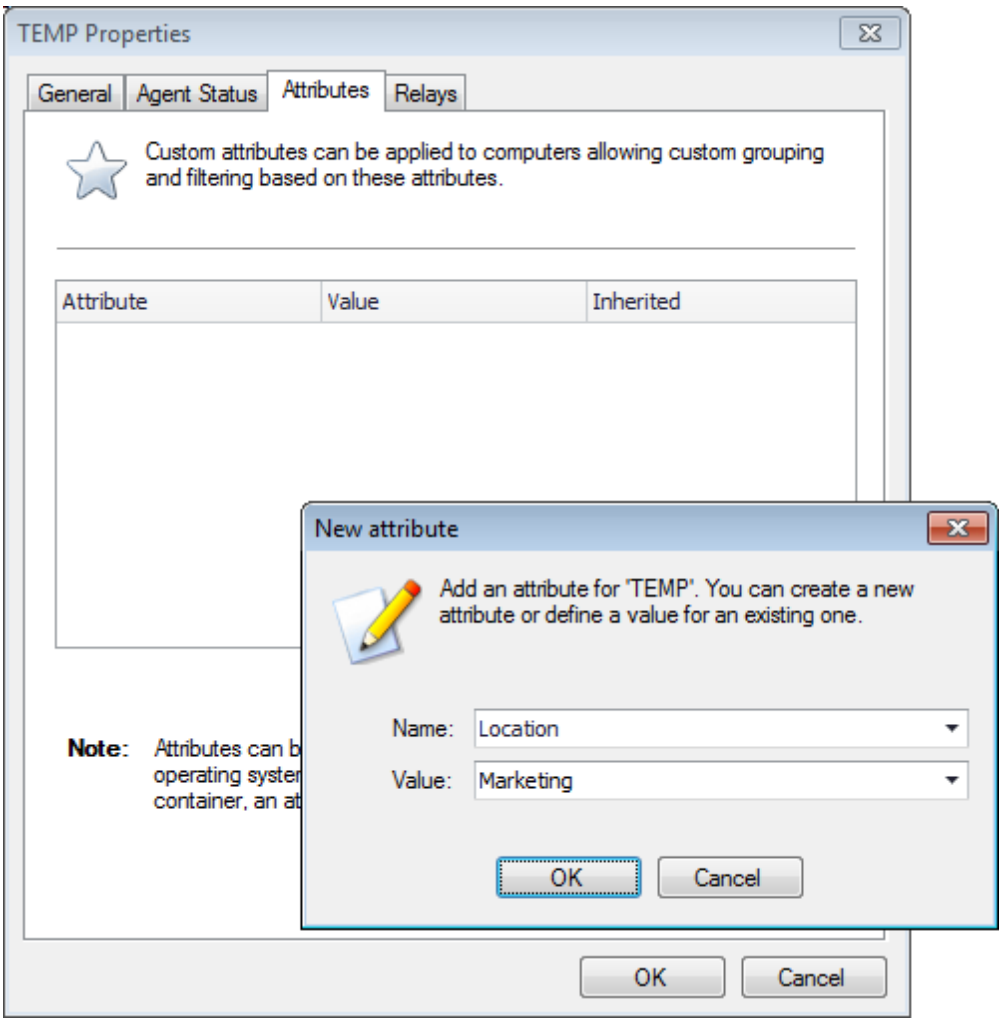
Opzione	Descrizione
Modifica pianificazione di scansione	Configura la pianificazione in base a cui GFI LanGuard esegue la ricerca di nuovi computer.
Profilo di scansione	Configura la pianificazione di controllo in base a cui vengono scansionati i computer di destinazione.
Impostazioni di riparazione automatica	Configurare le azioni di riparazione automatica da eseguire su tutti i computer di questo gruppo. For more information, refer to Configurazione della riparazione automatica agenti (page 141).

4. Selezionare **Individuazione della rete** e configurare le opzioni seguenti:

Table 22: Individuazione di rete gruppo agente

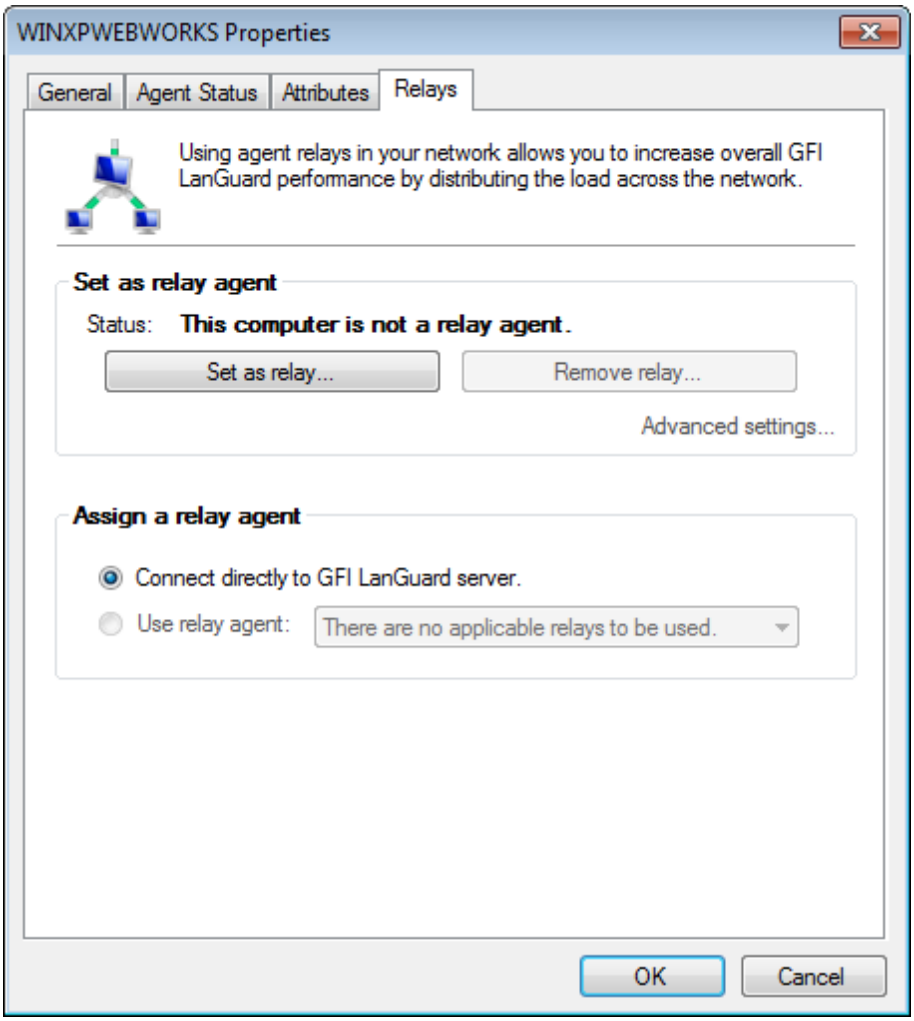
Opzione	Descrizione
Controlla automaticamente la presenza di nuovi computer in questo gruppo	GFI LanGuard cercherà automaticamente nuovi computer.
Cambia pianificazione	Modifica la pianificazione in base alla quale GFI LanGuard esegue la ricerca di nuovi computer.
Esegui adesso	Esegue l'individuazione di rete.
Scansione ricorsiva UO	In modo ricorsivo, esegue il ciclo attraverso tutte le unità organizzative e registra i computer.

5. Selezionare la scheda **Attributi** per gestire gli attributi assegnati al computer selezionato. Per gestire gli attributi, utilizzare i pulsanti **Aggiungi**, **Modifica** e **Rimuovi**.



Screenshot 29: Attributi agente

6. Per configurare i relay degli agenti, fare clic sulla scheda **Relay**. I relay consentono ai computer diversi da quello che ospita GFI LanGuard di agire come server di GFI LanGuard. Ciò consente di bilanciare il carico del traffico diretto a quel computer e di ottimizzare le prestazioni di scansione della rete.


WINXPWEBWORKS Properties
General
Agent Status
Attributes
Relays
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.
Set as relay agent
Status: This computer is not a relay agent.
Set as relay...
Remove relay...
Advanced settings...
Assign a relay agent
Connect directly to GFI LanGuard server.
Use relay agent:
There are no applicable relays to be used.
OK
Cancel

Screenshot 30: Relay agente

7. Configurare le opzioni descritte di seguito:

Table 23: Opzioni relay agente

Opzione	Descrizione
Connetti direttamente al server GFI LanGuard	Il computer selezionato scaricherà gli aggiornamenti del prodotto e le patch dal server di GFI LanGuard.
Usa agente relay	Il computer selezionato utilizzerà un agente relay per scaricare gli aggiornamenti del prodotto e le patch. Nell'elenco a discesa, selezionare l'agente relay da utilizzare.

Nota

Alcune opzioni sono disabilitate perché sono applicabili solo per i singoli computer.

8. Fare clic su **OK**.

5 Scansione della rete

Questo capitolo descrive le informazioni sulle modalità dei diversi profili di scansione supportate da GFI LanGuard, così come innestare scansioni manuali immediate o schedulate. Usare i metodi di scansione appropriati (usando le scansioni senza agente o basate su agente) in base alla disponibilità e alla posizione delle destinazioni di scansione.

Argomenti del presente capitolo:

5.1 Informazioni sui profili di scansione 65
5.2 Profili di scansione disponibili 65
5.3 Scansioni manuali 67
5.4 Abilitazione dei criteri di controllo di protezione 71
5.5 Scansioni pianificate 72
5.6 Scansioni pianificate agente 82

5.1 Informazioni sui profili di scansione

GFI LanGuard permette di eseguire la scansione dell'infrastruttura IT alla ricerca di particolari vulnerabilità utilizzando insiemi di controlli preconfigurati chiamati profili di scansione. I profili di scansione permettono di eseguire la scansione delle destinazioni di rete ed enumerare solamente informazioni specifiche. Ad esempio, si potrebbe voler usare un profilo di scansione configurato in modo da eseguire la scansione sui computer della DMZ piuttosto che sulla rete interna in uso.

In pratica, i profili di scansione permettono di concentrare le attività di scansione delle vulnerabilità su determinate aree dell'infrastruttura IT, come nel caso in cui si vogliano identificare esclusivamente gli aggiornamenti di sicurezza mancanti. Il vantaggio risiede nella riduzione della quantità di dati dei risultati di scansione da analizzare, restringendo la portata dell'indagine e aiutando a localizzare rapidamente le informazioni necessarie con maggior facilità.

Mediante i diversi profili di scansione, è possibile svolgere vari controlli di sicurezza di rete senza dover rieseguire il processo di riconfigurazione per ciascun tipo di scansione di sicurezza necessario.

5.2 Profili di scansione disponibili

GFI LanGuard viene fornito con i profili di scansione predefiniti descritti nelle sezioni che seguono. Per creare i propri profili di scansione personalizzati, fare riferimento a Creazione di un nuovo profilo di scansione. Utilizzare le informazioni contenute nelle sezioni seguenti per comprendere quali sono gli elementi rilevati da ciascun profilo di scansione sulle destinazioni di scansione:

- Profili di scansioni complete/combinate
- Profili di valutazione delle vulnerabilità
- Profili Controllo rete e software

5.2.1 Scansioni complete/combinate

Table 24: Profili di scansioni complete/combinate

Profili di scansioni complete/combinate	
Valutazione completa delle vulnerabilità	Usare questo profilo di scansione per enumerare specifiche vulnerabilità di rete, quali le porte TCP/UDP aperte solitamente sfruttate dai trojan, le patch e i service pack mancanti. L'elenco delle vulnerabilità enumerate da questo profilo può essere personalizzato all'interno della scheda Vulnerabilità. Le periferiche USB e le applicazioni installate non sono enumerate da questo profilo. Il profilo eseguirà la scansione di tutte le vulnerabilità, Sono comprese le vulnerabilità a cui è associata una patch Microsoft® e che sono considerate patch mancanti.
Scansione completa (attiva)	Usare questo profilo di scansione per recuperare le informazioni di sistema ed eseguire la scansione sulla rete per tutte le vulnerabilità supportate, comprese: porte TCP/UDP aperte, patch e service pack mancanti, periferiche USB connesse e altro. I time-out per il controllo delle vulnerabilità in questo profilo sono preconfigurati specificatamente per adattarsi al traffico di rete e ai ritardi di trasmissione solitamente associati agli ambienti LAN.
Scansione completa (reti lente)	Usare questo profilo di scansione per recuperare le informazioni di sistema ed eseguire la scansione sulla rete per tutte le vulnerabilità supportate, comprese:porte TCP/UDP aperte, patch e service pack mancanti, periferiche USB connesse e altro... I time-out per il controllo delle vulnerabilità in questo profilo sono preconfigurati specificatamente per adattarsi al traffico di rete e ai ritardi di trasmissione solitamente associati agli ambienti WAN.

5.2.2 Valutazione delle vulnerabilità

Table 25: Profili di scansione per la valutazione delle vulnerabilità

Profili di valutazione delle vulnerabilità	
Top 20 del SANS delle vulnerabilità	Usare questo profilo di scansione per enumerare tutte le vulnerabilità riportate nell'elenco Top 20 del SANS.
Vulnerabilità di sicurezza di livello alto	Usare questo profilo di scansione per enumerare le porte TCP/UDP aperte e le vulnerabilità di sicurezza di livello alto. L'elenco delle porte TCP/UDP e delle vulnerabilità di sicurezza di livello alto enumerate da questo profilo può essere personalizzato all'interno delle schede Porte TCP/UDP e Vulnerabilità.
Vulnerabilità dello scorso anno	Usare questo profilo di scansione per enumerare le vulnerabilità di rete emerse negli ultimi 12 mesi.
Solo Web	Usare questo profilo di scansione per identificare le vulnerabilità specifiche del server Web. Questa operazione comprende la scansione e l'enumerazione delle porte TCP usate più di frequente dai server Web come la porta 80. Solo le porte TCP comunemente usate dai server Web vengono sottoposte a scansione da questo profilo. Le operazioni di controllo di rete e l'enumerazione delle vulnerabilità e delle patch mancanti non possono essere eseguite utilizzando questo profilo.
Patch mancanti	Usare questo profilo di scansione per enumerare le patch mancanti. L'elenco di patch mancanti enumerate da questo profilo può essere personalizzato all'interno della scheda Patch.
Patch critiche	Usare questo profilo di scansione per enumerare solo le patch mancanti contrassegnate come critiche. L'elenco di patch critiche enumerate da questo profilo può essere personalizzato all'interno della scheda Patch.
Patch del mese scorso	Usare questo profilo di scansione per enumerare solo le patch mancanti rilasciate il mese precedente. L'elenco di patch mancanti enumerate da questo profilo può essere personalizzato all'interno della scheda Patch.
Solo service pack	Usare questo profilo di scansione per enumerare i service pack mancanti. L'elenco di service pack enumerati da questo profilo può essere personalizzato all'interno della scheda Patch.
Patch non Microsoft®	Usare questo profilo di scansione per enumerare le patch di terzi mancanti, quali i prodotti di Adobe.
Patch di protezione	Usare questo profilo di scansione per enumerare le patch di protezione Microsoft® e non Microsoft® mancanti sulle destinazioni di scansione.

5.2.3 Controllo rete e software

Table 26: Controllo rete e software

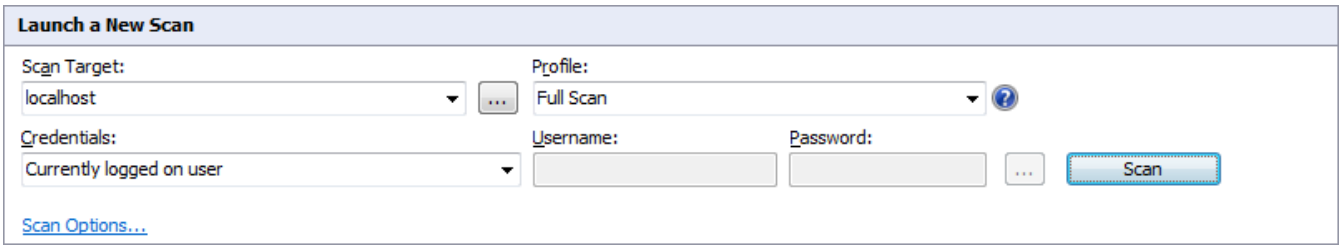
Profili di controllo rete e software	
Porte trojan	Usare questo profilo di scansione per enumerare le porte TCP/UDP aperte comunemente sfruttate da noti trojan. L'elenco di porte TCP/UDP da sottoporre a scansione può essere personalizzato all'interno delle rispettive schede Porte TCP e Porte UDP. Questo profilo esegue la scansione solo sulle porte TCP/UDP comunemente sfruttate da noti trojan. Le operazioni di controllo di rete e l'enumerazione delle porte TCP/UDP aperte e delle patch mancanti non possono essere eseguite da questo profilo.
Scanner per porte	Usare questo profilo di scansione per enumerare le porte TCP/UDP aperte comprese quelle più comunemente sfruttate dai trojan. L'elenco di porte enumerate da questo profilo può essere personalizzato all'interno della scheda Porte TCP/UDP.
Controllo software	Usare questo profilo di scansione per enumerare tutte le applicazioni software installate sulle destinazioni delle scansioni. Queste comprendono software di sicurezza come software antivirus e antispyware.
Scansione completa TCP e UDP	Usare questo profilo di scansione per controllare la rete ed enumerare tutte le porte TCP e UDP aperte.
Solo SNMP	Usare questo profilo di scansione per rilevare e recuperare le informazioni sulla rete riguardanti i dispositivi hardware (router, interruttori, stampanti, ecc.) con SNMP abilitato. Questa operazione consente di monitorare i dispositivi collegati alla rete per i casi che richiedono attenzione da parte dell'amministrazione.
Esegue il ping di tutti	Usare questo profilo di scansione per controllare la rete ed enumerare tutti i computer attualmente connessi e in esecuzione.
Trova condivisioni	Usare questo profilo di scansione per controllare la rete ed enumerare tutte le condivisioni aperte, visibili o nascoste. Questo profilo non esegue alcun controllo delle vulnerabilità.
Tempi di attività	Usare questo profilo di scansione per controllare la rete e identificare per quanto tempo ogni singolo computer è rimasto in esecuzione dall'ultimo avvio.
Utilizzo dello spazio su disco	Usare questo profilo di scansione per controllare la rete e recuperare le informazioni di sistema sullo spazio di archiviazione disponibile.
Informazioni di sistema	Usare questo profilo di scansione per recuperare le informazioni di sistema come i dettagli del sistema operativo, i dispositivi di rete wireless/virtuali/fisici connessi, le periferiche USB collegate, le applicazioni installate e altro.
Verifica hardware	Usare questo profilo di scansione per controllare la rete ed enumerare tutti i dispositivi hardware attualmente collegati ai computer della rete in uso.
Individuazione di rete	Usare questo profilo di scansione per enumerare qualsiasi dispositivo con il protocollo IP abilitato che è connesso alla rete.

5.3 Scansioni manuali

La scansione manuale è un processo che prevede l'esecuzione di controlli sui computer di destinazione senza l'intervento di agenti. Per effettuare una scansione manuale su un computer specifico:

1. Avviare GFI LanGuard.

2. Dalla scheda **Home**, selezionare **Avvia una scansione**. In alternativa fare clic sulla scheda **Scansione**.



Screenshot 31: Impostazioni Scansione manuale

3. Dal menu a discesa **Scansiona destinazione**, selezionare il computer di destinazione o il gruppo di computer da scansionare utilizzando le seguenti opzioni:

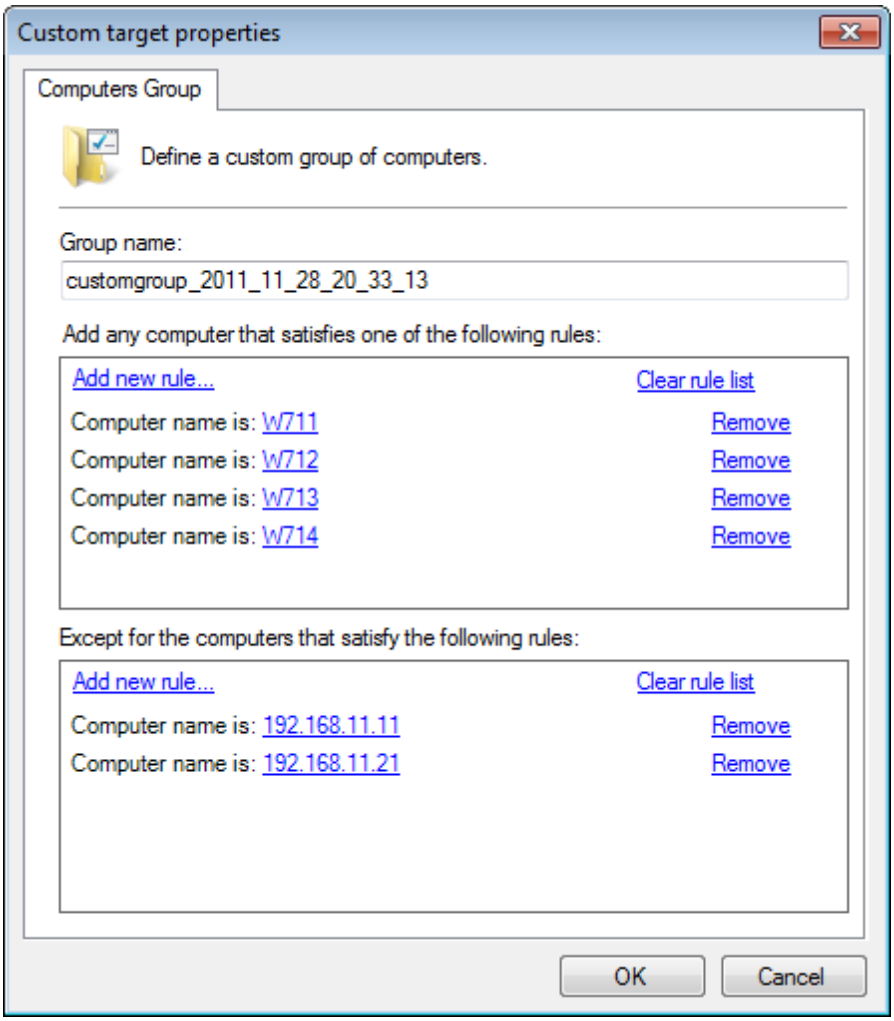
Table 27: Opzioni computer di destinazione durante il controllo

Opzione	Descrizione
Localhost	Controlla l'host locale dove è installato GFI LanGuard.
Dominio: dominio primario	Controlla l'intero dominio/gruppo di lavoro del computer/server dove è installato GFI LanGuard.

Nota

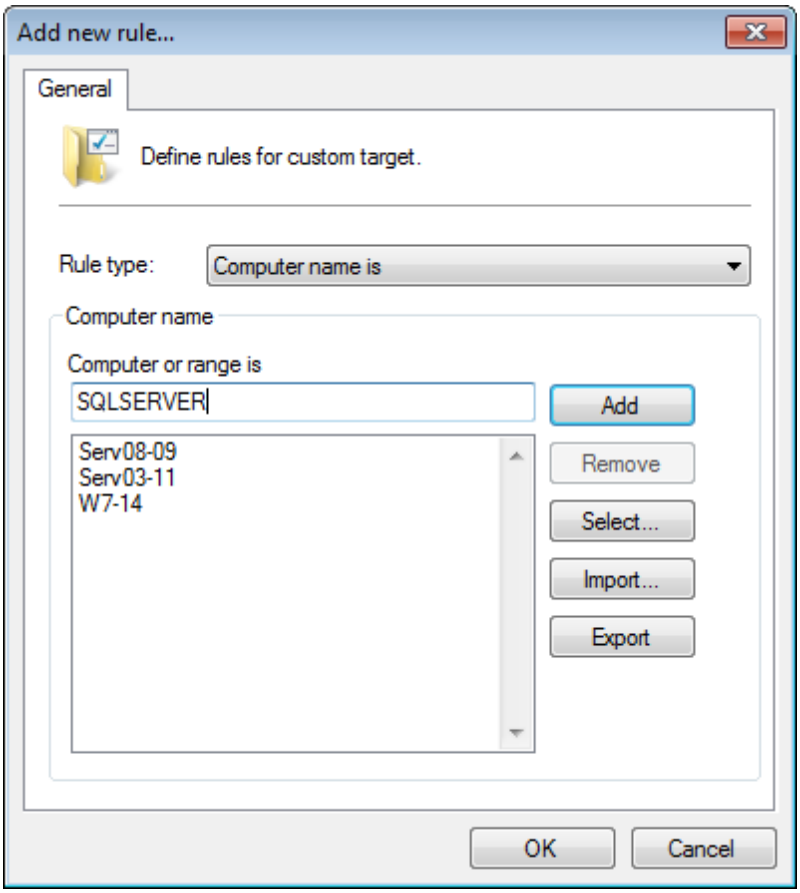
In via opzionale, dalla struttura computer fare clic con il pulsante destro del mouse su un computer/gruppo di computer e selezionare **Scansione > Scansione personalizzata**.

4. Fare clic sul pulsante Sfoglia (**...**) per definire le regole personalizzate per l'aggiunta delle destinazioni di scansione.



Screenshot 32: Proprietà personalizzate destinazione

5. Dalla finestra di dialogo **Proprietà personalizzate destinazione** fare clic sui collegamenti **Aggiungi nuova regola** per creare una regola personalizzata per i computer che si desidera sottoporre a scansione oppure escludere dalla scansione.



Screenshot 33: Aggiungi nuova regola...

6. Dalla finestra di dialogo **Aggiungi nuova regola** selezionare il **Tipo di regola** descritto in basso per l'aggiunta di computer:

Table 28: Proprietà personalizzate destinazione

Tipo di regola	Descrizione
Nome computer è	Cerca e aggiunge i computer in base al nome. Digitare un nome computer valido e fare clic su **Aggiungi** per ogni computer. Per applicare le modifiche fare clic su **OK**.
L'elenco file computer è	Cerca e aggiunge i computer da un file di testo. Fare clic sul pulsante Sfoglia e individuare il file di testo. Per applicare le modifiche fare clic su **OK**. **Nota** Quando si invia un elenco di computer di destinazione da un file, assicurarsi che il file contenga un solo nome di computer di destinazione per riga.
Nome dominio è	Cerca e aggiunge i computer che sono membri del dominio. Selezionare i domini dall'elenco e fare clic su **OK**.
L'indirizzo IP è	Cerca e aggiunge i computer in base all'indirizzo IP. Selezionare **Questo computer** per aggiungere l'host locale o **Esegui la scansione su un altro computer** per aggiungere un computer remoto. Digitare l'indirizzo IP se richiesto e fare clic su **OK**.
L'intervallo indirizzi IP è	Cerca e aggiunge i computer compresi in un intervallo IP. Selezionare **Scansiona un intervallo indirizzi IP** e digitare l'intervallo di indirizzi IP o selezionare Subnet CIDR e digitare l'intervallo con notazione CIDR. **Nota** Il CIDR (Classless Inter-Domain Routing) fornisce una soluzione alternativa per indicare un intervallo IP specifico. La notazione è la seguente: `<Indirizzo di base> / <Prefisso rete IP>`. Esempio: 192.168.0.0/16

Tipo di regola	Descrizione
Unità organizzativa è	Cerca e aggiunge i computer di un'unità organizzativa. Fare clic su **Seleziona** e dall'elenco selezionare le unità organizzative. Fare clic su **OK**.

7. Una volta aggiunte le regole, fare clic su **OK** per chiudere la finestra di dialogo **Aggiungi nuova regola**. Fare clic su **OK** per chiudere la finestra di dialogo **Proprietà personalizzate destinazione** e tornare alle impostazioni di scansione.

8. Dal menu a discesa **Profilo**, selezionare il profilo di scansione che GFI LanGuard dovrà attivare durante la scansione. For more information, refer to Profili di scansione disponibili (page 65).

9. Dal menu a discesa **Credenziali** selezionare il metodo di accesso utilizzato da GFI LanGuard per collegarsi alle destinazioni di scansione. La sottostante tabella illustra le opzioni disponibili:

Table 29: Opzioni di accesso e di controllo

Opzione	Descrizione
Utente attualmente connesso	Utilizza le credenziali dell'utente attualmente connesso al momento di accedere alle destinazioni di scansione.
Credenziali alternative	Utilizza le credenziali personalizzate. Digitare il nome utente e la password da utilizzare.
Una sessione nulla	Accede alle destinazioni di scansione utilizzando una sessione nulla. L'utente accederà al computer di destinazione come utente anonimo.
Un file chiave privata	Accede ai computer UNIX tramite SSH. È necessario immettere un nome utente e una password.

> **Nota**
>
> Le credenziali fornite devono disporre di privilegi di amministratore per consentire a GFI LanGuard di accedere ai computer di destinazione ed effettuare il controllo di rete.

10. (Facoltativo) Fare clic su **Opzioni di scansione** e configurare le opzioni descritte di seguito:

Table 30: Opzioni di scansione

Opzione	Descrizione
Utilizza credenziali computer se disponibili	Per accedere ai computer di destinazione specificati tramite le credenziali del Dashboard.
Ricorda credenziali	Per utilizzare le credenziali configurate come predefinite per l'esecuzione di un controllo.
Attiva i computer non in linea	GFI LanGuard tenta di alimentare i computer non in linea utilizzando la Wake-on-LAN. For more information, refer to Configurazione di Wake-on-LAN sulle destinazioni di scansione (page 135).
Arresta i computer dopo la scansione	Esegue l'arresto al completamento della scansione.

11. Per avviare il controllo delle destinazioni selezionate, fare clic su **Scansione**.

5.4 Abilitazione dei criteri di controllo di protezione

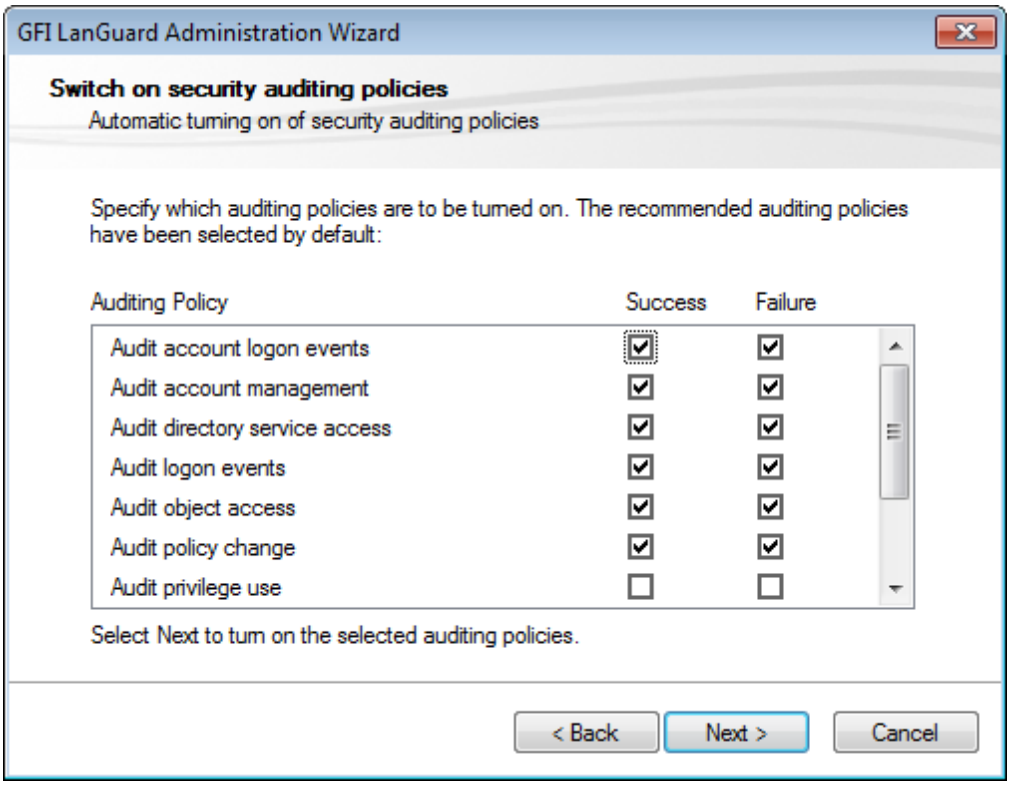
Una componente importante di qualsiasi piano di sicurezza è l'abilità di monitorare e controllare gli eventi che si verificano sulla rete in uso. I registri di eventi vengono consultati di frequente al fine di identificare le falle o i buchi di sicurezza. È di fondamentale importanza identificare i tentativi di violazione della sicurezza del sistema e impedirne il successo. All'interno di Windows, è possibile usare

per configurare un criterio di controllo avente lo scopo di tracciare le attività degli utenti o gli eventi del sistema all'interno di specifici registri.

Per tracciare i criteri di controllo di sistema, GFI LanGuard raccoglie le impostazioni dei criteri di controllo di protezione dai computer di destinazione e li inserisce nei risultati della scansione. Per accedere a più informazioni sui risultati, selezionare il sottonodo **Criterio controllo di protezione**.

Oltre ad acquisire informazioni sulle impostazioni correnti dei criteri di controllo, è possibile utilizzare anche GFI LanGuard per accedere e modificare le impostazioni dei criteri di controllo dei computer di destinazione. A tal fine:

1. Dopo aver scansionato un computer remoto, dal pannello **Panoramica risultati di scansione**, fare clic con il tasto destro del mouse sul relativo computer di destinazione e selezionare **Attiva Controllo su** > **Computer in uso/computer selezionati/tutti i computer**.


GFI LanGuard Administration Wizard
Switch on security auditing policies
Automatic turning on of security auditing policies
Specify which auditing policies are to be turned on. The recommended auditing policies have been selected by default:
Auditing Policy
Success
Failure
Audit account logon events
Audit account management
Audit directory service access
Audit logon events
Audit object access
Audit policy change
Audit privilege use
Select Next to turn on the selected auditing policies.
< Back
Next >
Cancel

Screenshot 34: Procedura guidata Amministrazione criteri di controllo

2. Selezionare/deselezionare i criteri di controllo a seconda della necessità e fare clic su **Avanti** per applicare le impostazioni della configurazione dei criteri di controllo al/ai computer di destinazione.

3. A questo punto, verrà visualizzata una finestra di dialogo che informa l'utente della riuscita o meno dell'applicazione delle impostazioni ai criteri di controllo. Per passare alla fase successiva, fare clic su **Avanti**. Per distribuire nuovamente le impostazioni nei computer dove non hanno avuto esito positivo, selezionare **Indietro**.

4. Per completare la configurazione, fare clic su **Fine**. Riavviare una scansione per aggiornare i risultati.

5.5 Scansioni pianificate

Una scansione pianificata è un controllo di rete pianificato in modo da essere eseguito automaticamente in un giorno/a un'ora specifici e con una determinata frequenza. Le scansioni pianificate possono essere impostate per essere eseguite una volta o periodicamente. Lo stato della scansione pianificata viene monitorato dalla scheda **Monitor attività>Scansioni di sicurezza**.

GFI consiglia le scansioni pianificate nei seguenti casi:

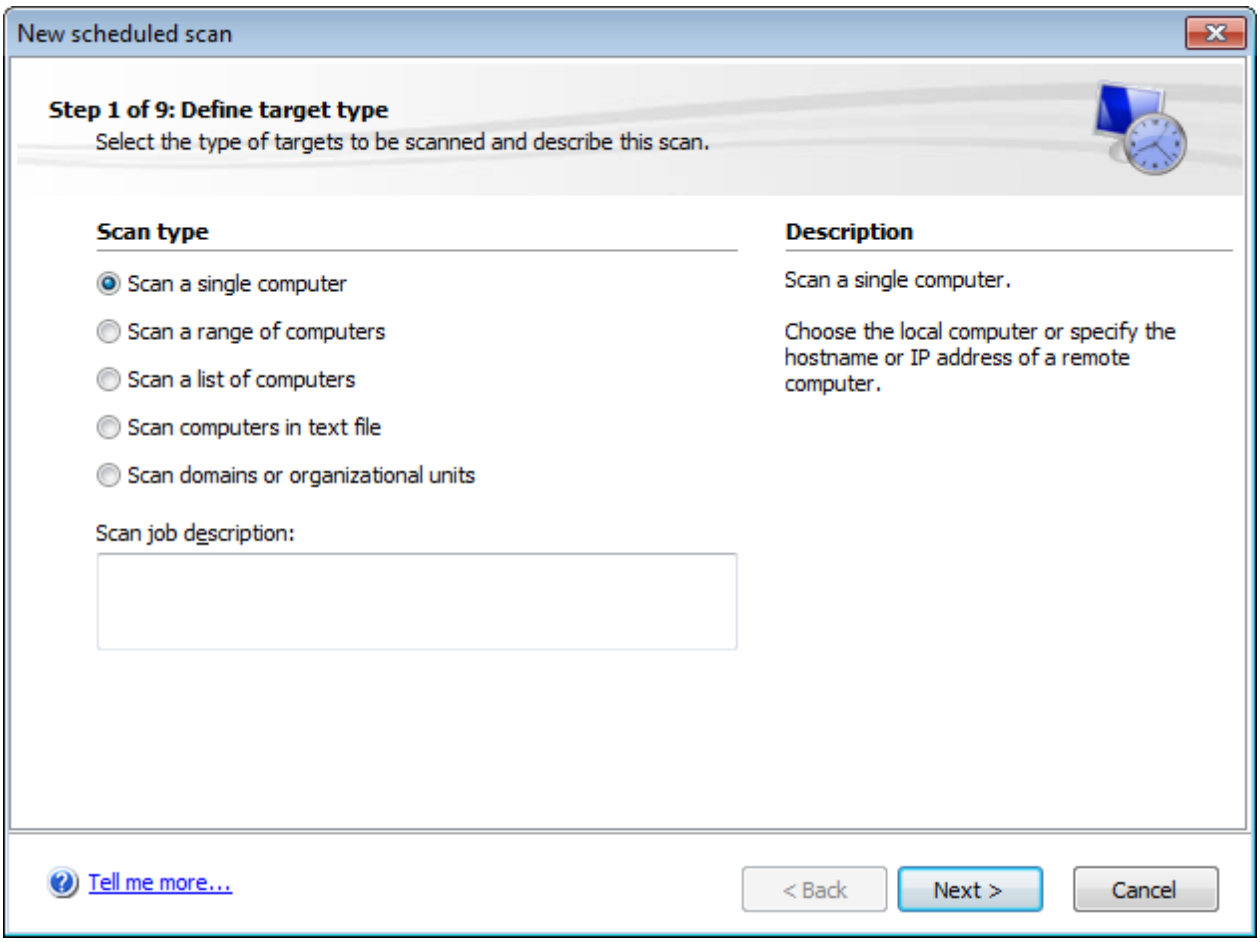
- Quando gli agenti GFI LanGuard non sono distribuiti nei computer di destinazione
- Per svolgere automaticamente scansioni periodiche/regolari delle vulnerabilità di rete utilizzando gli stessi profili.
- Per avviare automaticamente le scansioni fuori dagli orari di lavoro e generare avvisi e distribuzioni automatiche dei risultati delle scansioni tramite posta elettronica
- Per attivare automaticamente le opzioni di riparazione automatica (ad es. download e distribuzione automatica degli aggiornamenti mancanti).

Le sezioni seguenti contengono informazioni che guideranno l'utente nella configurazione e nell'esecuzione delle scansioni pianificate:

- Creazione di una scansione pianificata
- Modifica impostazioni scansione pianificata
- Configurazione proprietà scansione pianificata

5.5.1 Creazione di una scansione pianificata

1. Avviare GFI LanGuard.
2. Fare clic sulla scheda **Configurazione>Scansioni pianificate**.
3. Da **Attività comuni**, selezionare **Nuova scansione pianificata**.


New scheduled scan
Step 1 of 9: Define target type
Select the type of targets to be scanned and describe this scan.
Scan type
Scan a single computer
Scan a range of computers
Scan a list of computers
Scan computers in text file
Scan domains or organizational units
Scan job description:
Description
Scan a single computer.
Choose the local computer or specify the hostname or IP address of a remote computer.
Tell me more...
< Back
Next >
Cancel

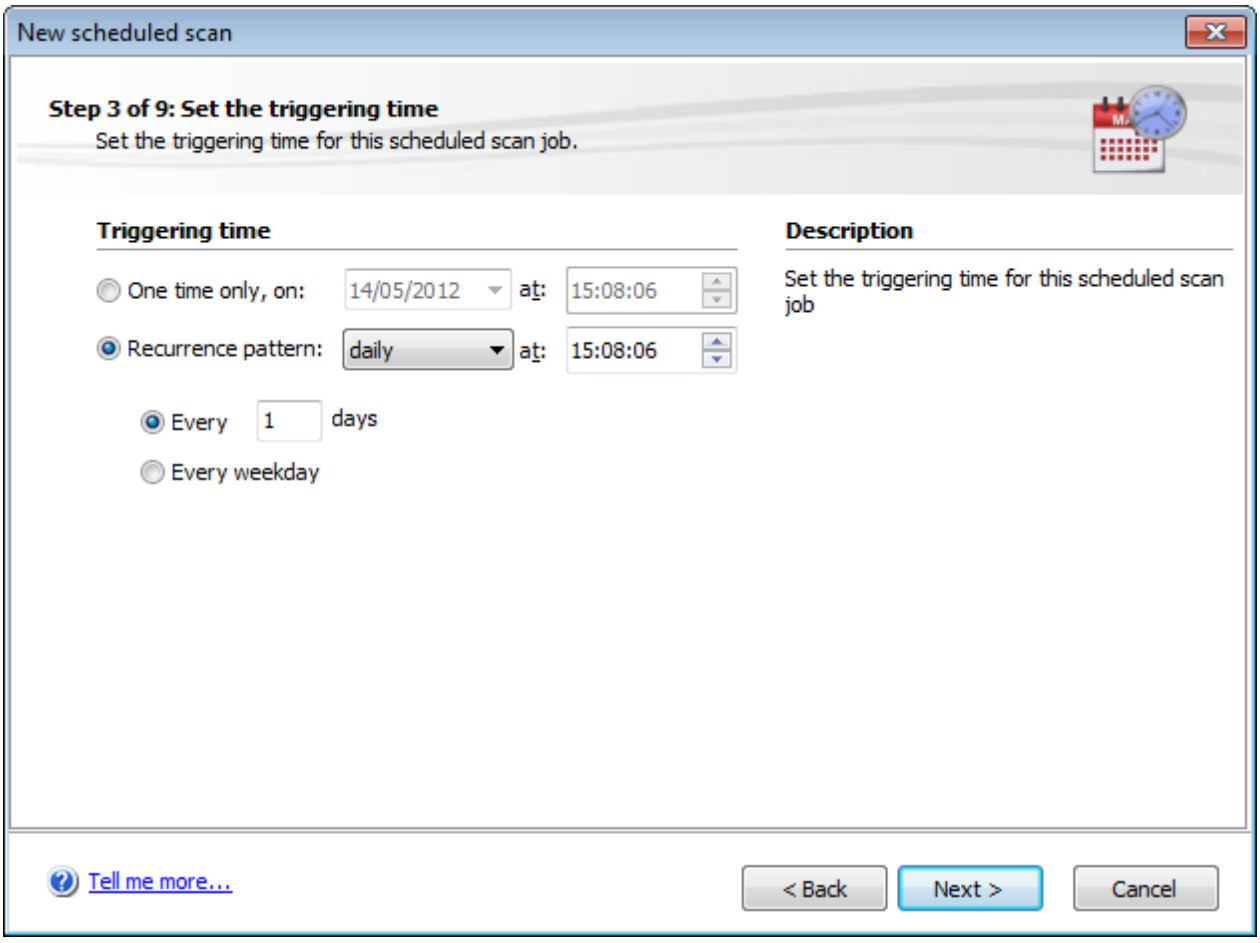
Screenshot 35: Finestra di dialogo Nuova scansione pianificata

4. Selezionare una delle opzioni descritte di seguito e fare clic su **Avanti**.

Table 31: Nuovo tipo di scansione pianificata

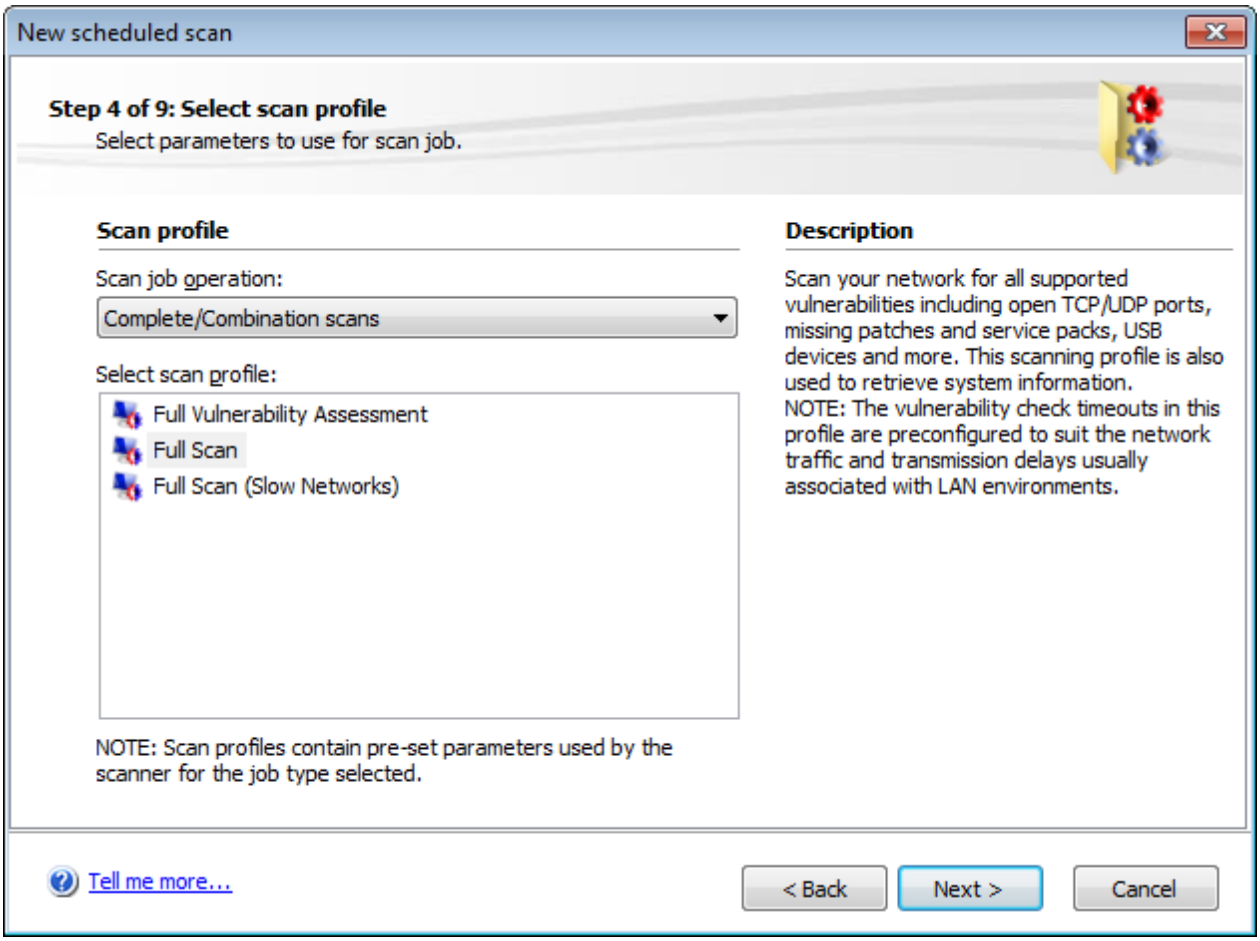
Opzione	Descrizione
Esegui la scansione su un unico computer	Scansiona l'host locale o un computer specifico.
Esegui la scansione su una serie di computer	Scansiona una serie di computer definiti per mezzo di un intervallo di IP.
Esegui la scansione di un elenco di computer	Crea manualmente un elenco di destinazioni, importa le destinazioni da un file oppure seleziona le destinazioni da un elenco di rete.
Esegui la scansione sui computer elencati in un file di testo	Scansiona le destinazioni elencate in uno specifico file di testo.
Scansione domini o unità organizzative	Scansiona tutte le destinazioni collegate a un dominio/un'unità organizzativa specificati.

5. A seconda dell'opzione selezionata nel passaggio precedente, indicare i dati dei rispettivi computer di destinazione e fare clic su **Avanti**.



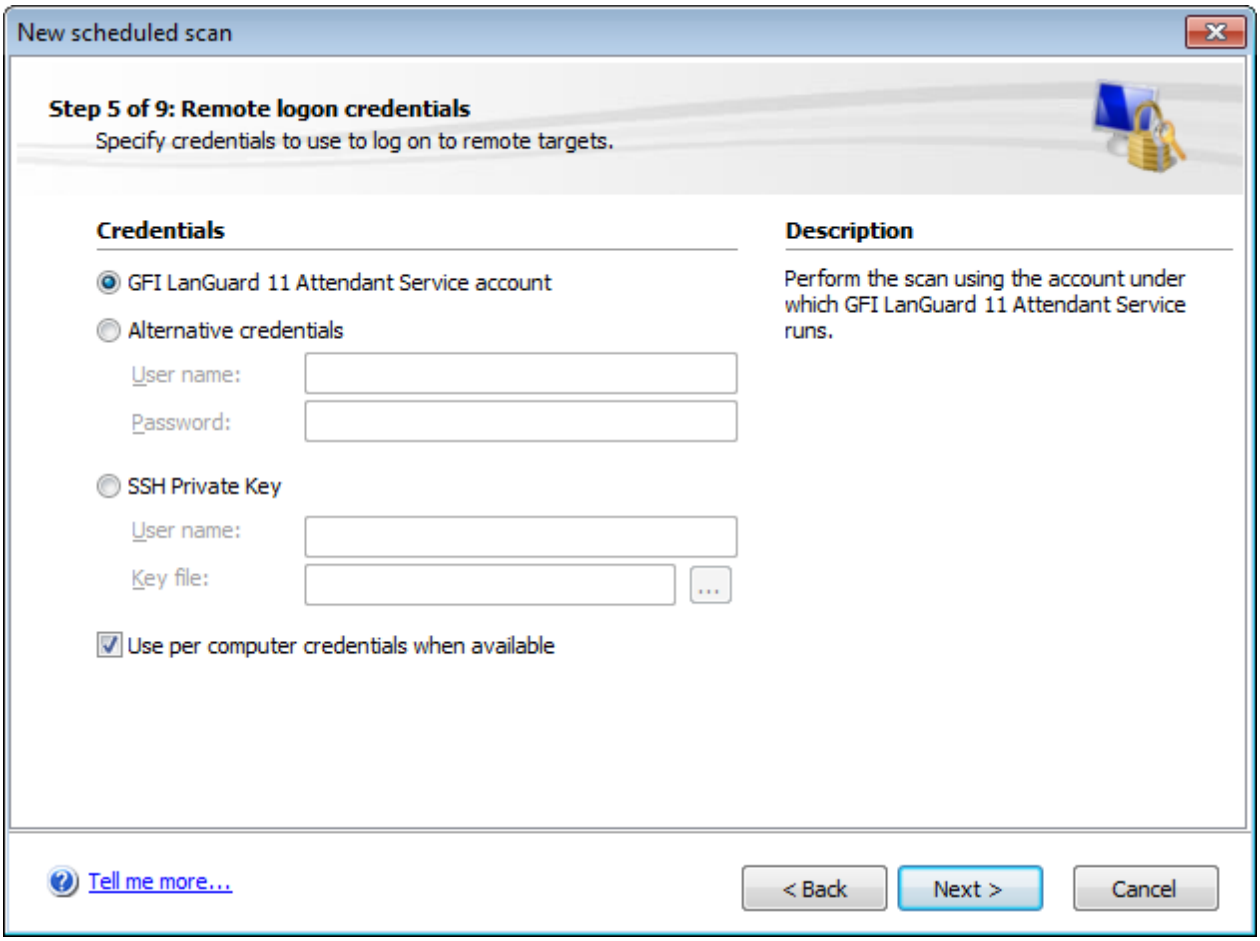
Screenshot 36: Frequenza scansione pianificata

6. Specificare la data/l'ora/la frequenza della nuova scansione pianificata, quindi fare clic su **Avanti**.


New scheduled scan
Step 4 of 9: Select scan profile
Select parameters to use for scan job.
Scan profile
Scan job operation:
Complete/Combination scans
Select scan profile:
Full Vulnerability Assessment
Full Scan
Full Scan (Slow Networks)
NOTE: Scan profiles contain pre-set parameters used by the scanner for the job type selected.
Description
Scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices and more. This scanning profile is also used to retrieve system information.
NOTE: The vulnerability check timeouts in this profile are preconfigured to suit the network traffic and transmission delays usually associated with LAN environments.
Tell me more...
< Back
Next >
Cancel

Screenshot 37: Scelta profilo di scansione

7. Dal menu a discesa **Operazione processo di scansione** selezionare il profilo di scansione da utilizzare durante la scansione, quindi fare clic su **Avanti**. For more information, refer to Profili di scansione disponibili (page 65).

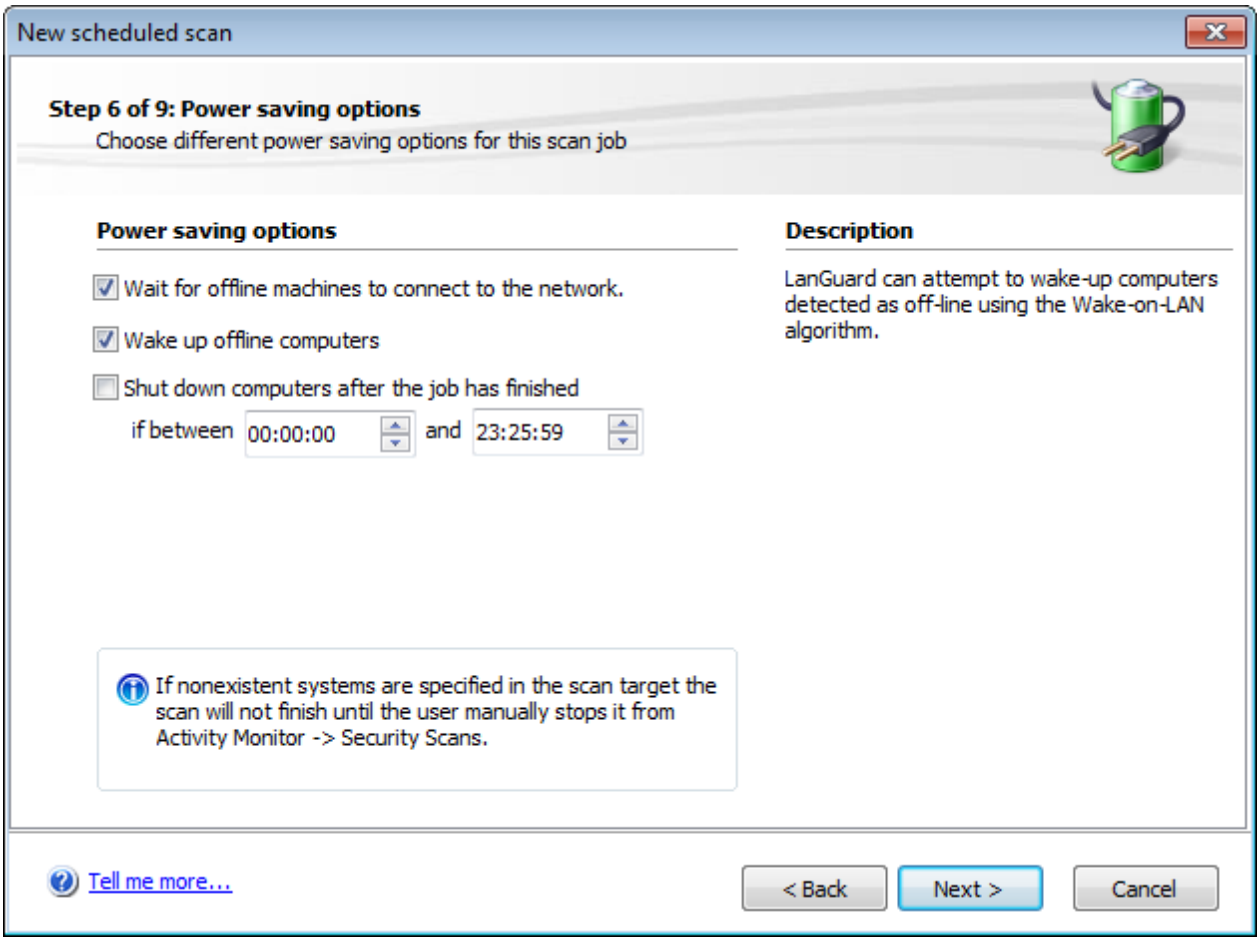


Screenshot 38: Credenziali di accesso remoto

8. (Facoltativo) Specificare le **Credenziali di accesso remoto** e fare clic su **Avanti**. Le credenziali di accesso remoto possono essere una delle seguenti opzioni:

Table 32: Credenziali di accesso remoto

Opzione	Descrizione
Account servizio GFI LanGuard 11 Attendant	Esegue la scansione utilizzando le credenziali specificate durante l'installazione di GFI LanGuard 2011.
Credenziali alternative	Specifica le credenziali alternative per la connessione ai computer per la scansione. **Nota** Assicurarsi che le credenziali fornite dispongano dei privilegi amministrativi.
Chiave SSH privata	Digitare un nome utente e selezionare il file chiave utilizzato per accedere ai sistemi basati su UNIX/LINUX.
Utilizza credenziali computer se disponibili	Utilizza le credenziali predefinite per la scansione configurata.

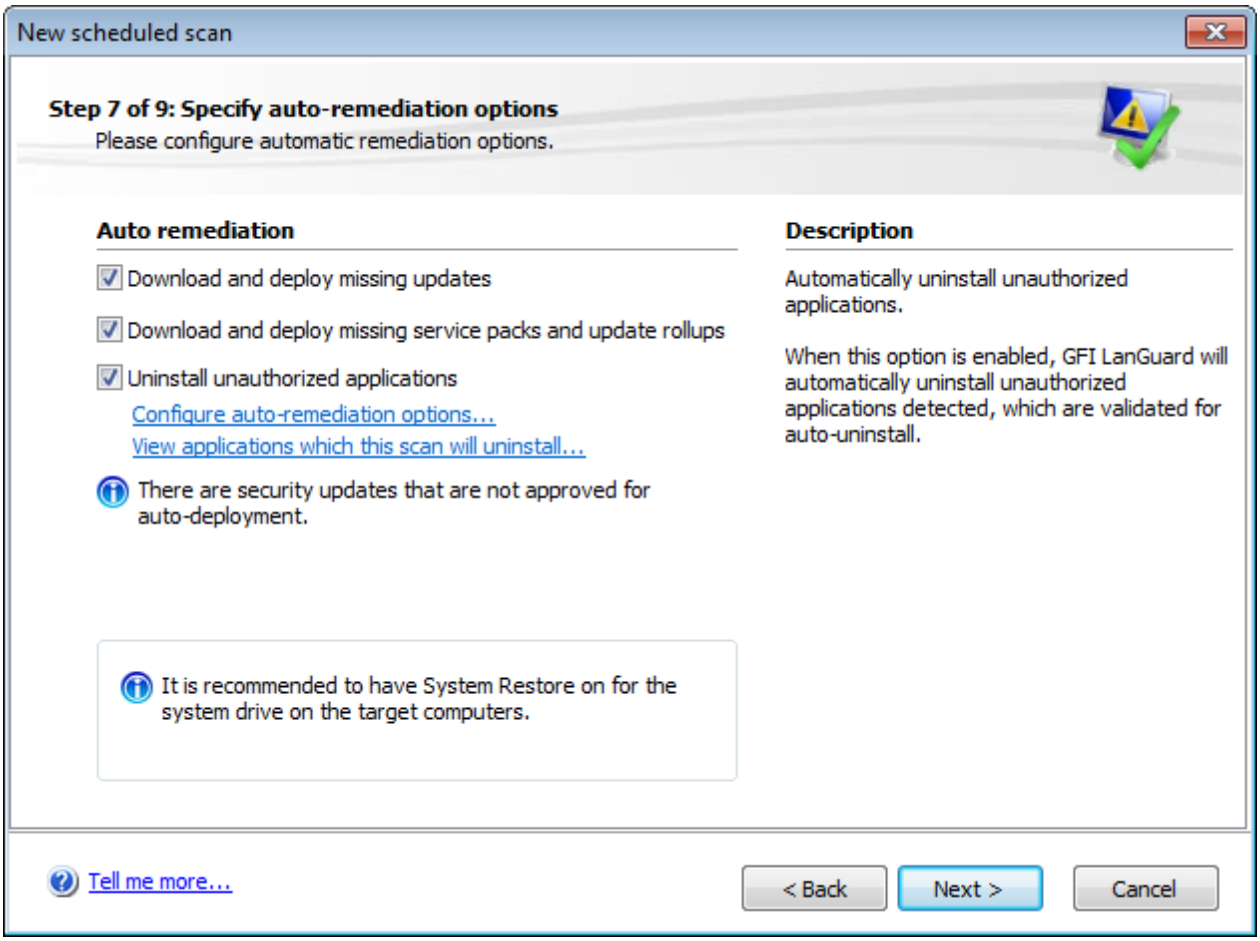

New scheduled scan
Step 6 of 9: Power saving options
Choose different power saving options for this scan job
Power saving options
Wait for offline machines to connect to the network.
Wake up offline computers
Shut down computers after the job has finished
if between 00:00:00 and 23:25:59
Description
LanGuard can attempt to wake-up computers detected as off-line using the Wake-on-LAN algorithm.
If nonexistent systems are specified in the scan target the scan will not finish until the user manually stops it from Activity Monitor -> Security Scans.
Tell me more...
< Back
Next >
Cancel

Screenshot 39: Opzioni di creazione dei rapporti della scansione pianificata

9. Dalle opzioni **Risparmio energetico**, configurare le seguenti opzioni:

Table 33: Opzioni di risparmio energetico

Opzione	Descrizione
Attendere la connessione alla rete dei computer offline	Arresta computer al termine dell'operazione
Tentare di attivare i computer non in linea	GFI LanGuard tenta di alimentare i computer non in linea utilizzando la Wake-on-LAN. For more information, refer to Configurazione di Wake-on-LAN sulle destinazioni di scansione (page 135).
Arresta computer al termine dell'operazione	Al termine della scansione di un computer o di un processo di riparazione automatica, GFI LanGuard tenta di arrestare il computer se l'orario rientra nell'intervallo specificato. **Nota** Se le opzioni di arresto sono definite nelle opzioni di riparazione automatica, le opzioni di risparmio energetico verranno ignorate.

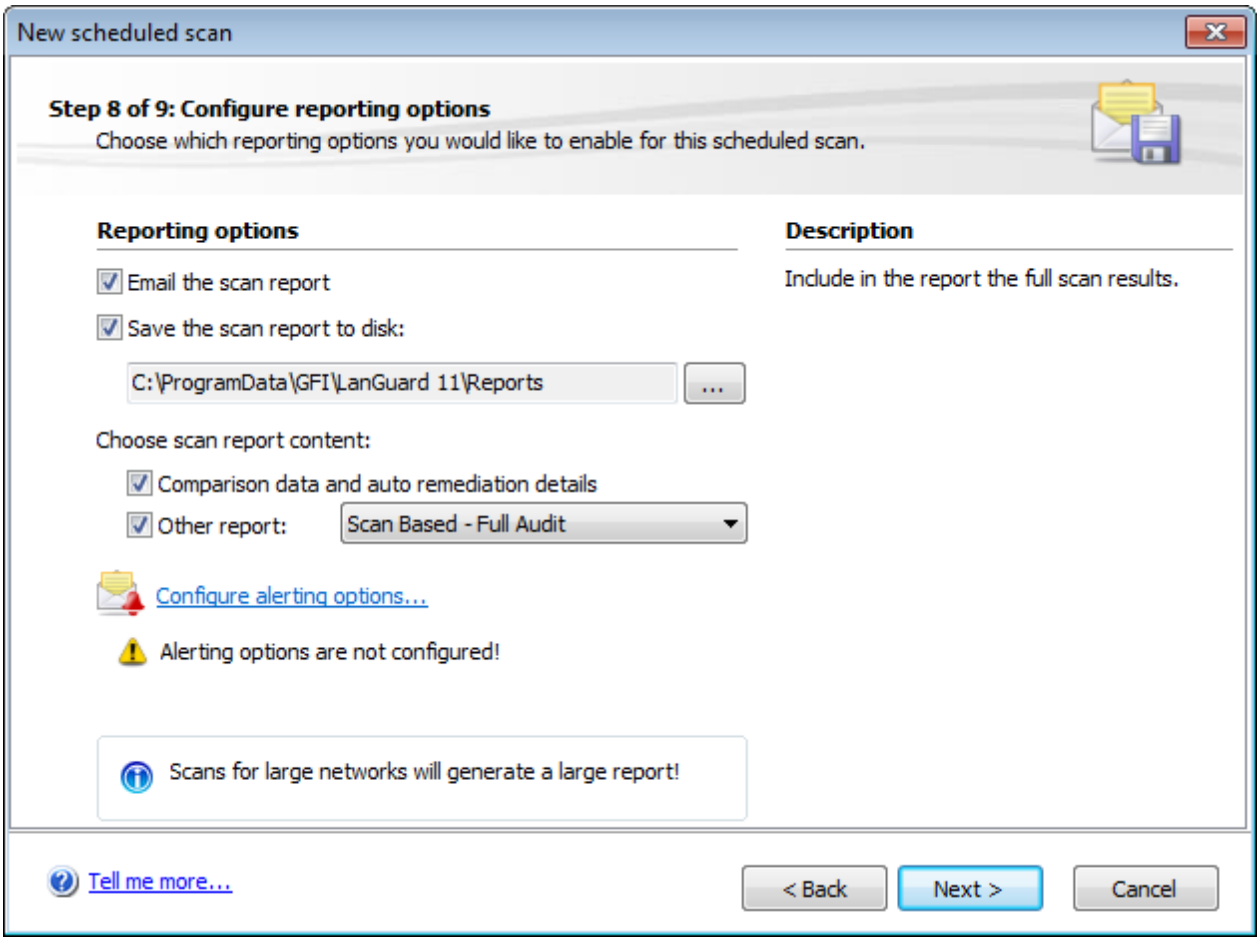

New scheduled scan
Step 7 of 9: Specify auto-remediation options
Please configure automatic remediation options.
Auto remediation
Download and deploy missing updates
Download and deploy missing service packs and update rollups
Uninstall unauthorized applications
Configure auto-remediation options...
View applications which this scan will uninstall...
There are security updates that are not approved for auto-deployment.
It is recommended to have System Restore on for the system drive on the target computers.
Description
Automatically uninstall unauthorized applications.
When this option is enabled, GFI LanGuard will automatically uninstall unauthorized applications detected, which are validated for auto-uninstall.
Tell me more...
< Back
Next >
Cancel

Screenshot 40: Opzioni di riparazione automatica della scansione pianificata

10. Dalla finestra di dialogo di riparazione automatica, selezionare le opzioni necessarie, quindi fare clic su **Avanti**. La sottostante tabella visualizza un elenco di opzioni disponibili:

Table 34: Opzioni di riparazione automatica

Opzione	Descrizione
Download e distribuzione degli aggiornamenti mancanti	Download e distribuzione automatica di patch mancanti nei computer di destinazione.
Download e distribuzione dei service pack e degli aggiornamenti cumulativi mancanti	Download e distribuzione automatica di service pack mancanti nei computer di destinazione.
Disinstallazione applicazioni non autorizzate	Se questa opzione è selezionata, tutte le applicazioni convalidate come non autorizzate verranno disinstallate dal computer sottoposto a scansione (le applicazioni non autorizzate sono riportate nella sezione Inventario applicazioni). For more information, refer to Configurazione della disinstallazione automatica delle applicazioni non autorizzate (page 126).
Configura riparazione automatica	Rimuove in automatico le applicazioni non autorizzate dai computer di destinazione. Le applicazioni non autorizzate sono definite nell'Inventario applicazioni. For more information, refer to Configurazione della disinstallazione automatica delle applicazioni non autorizzate (page 126).
Visualizza le applicazioni che verranno disinstallate	Fare clic sul collegamento per avviare la finestra di dialogo Applicazioni che verranno disinstallate. Si aprirà un elenco di tutte le applicazioni che verranno disinstallate al termine della scansione pianificata.

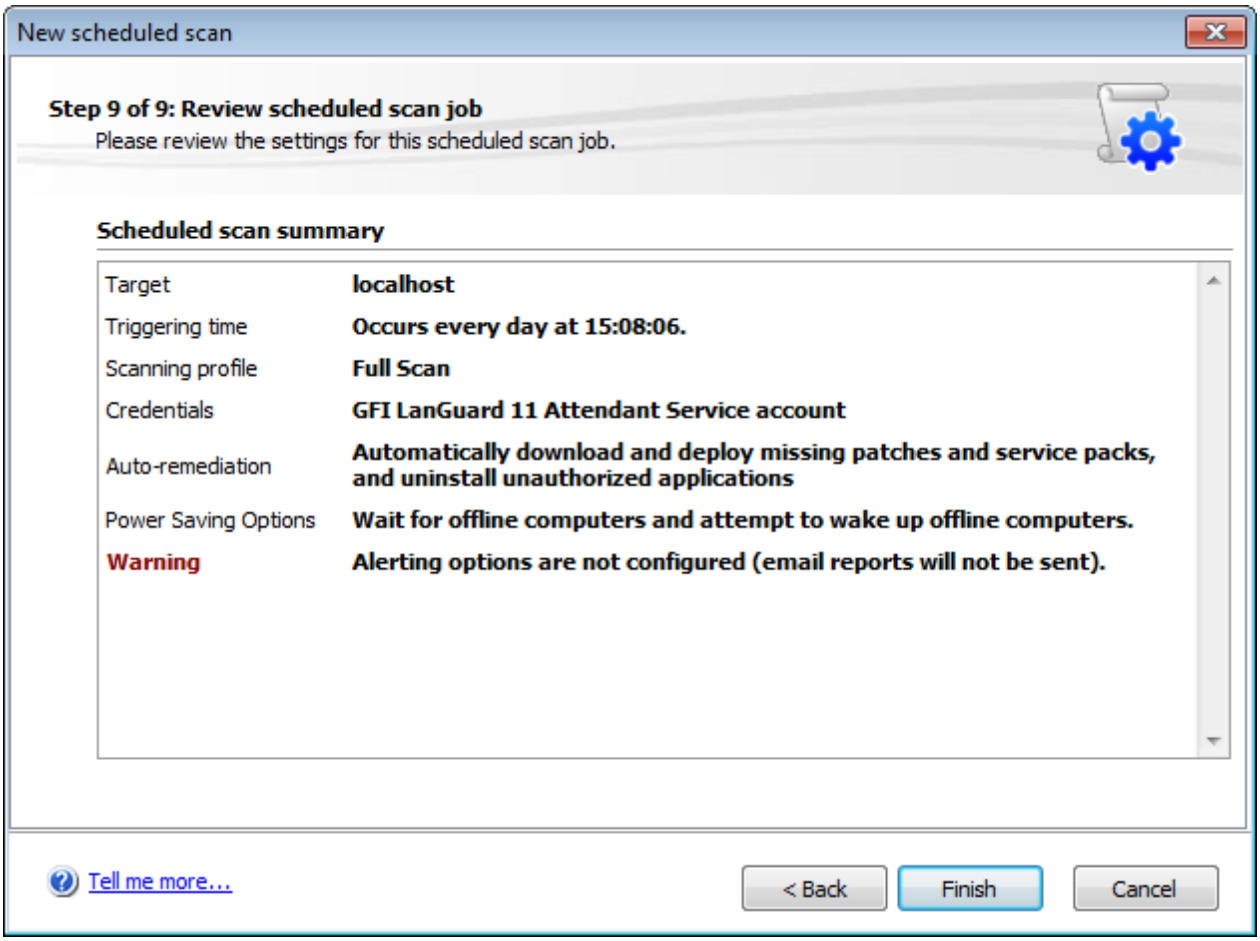

New scheduled scan
Step 8 of 9: Configure reporting options
Choose which reporting options you would like to enable for this scheduled scan.
Reporting options
Description
Email the scan report
Include in the report the full scan results.
Save the scan report to disk:
C:\ProgramData\GFI\LanGuard 11\Reports
...
Choose scan report content:
Comparison data and auto remediation details
Other report:
Scan Based - Full Audit
Configure alerting options...
Alerting options are not configured!
Scans for large networks will generate a large report!
Tell me more...
< Back
Next >
Cancel

Screenshot 41: Opzioni di creazione dei rapporti della scansione pianificata

11. (Facoltativo) Configurare le **opzioni di creazione di rapporti** come descritto di seguito:

Table 35: Opzioni di creazione dei rapporti

Opzione	Descrizione
Invia per e-mail il rapporto di scansione	Invia un rapporto tramite posta elettronica al termine di ciascuna scansione pianificata.
Salva il rapporto di scansione su disco	Salva il rapporto sul disco al termine di ciascuna scansione pianificata
Dati di confronto e dettagli di riparazione automatica	Include i dettagli delle operazioni di riparazione automatica e il confronto dei risultati con le scansioni di sicurezza precedenti. **Nota** Il confronto viene eseguito tra le scansioni con le stesse destinazioni di scansione e il profilo di scansione.
Dati dei risultati di scansione completa	Include i dettagli dei risultati della scansione completa.
Configurazione delle opzioni di avviso	(Facoltativo) Fare clic su Configurazione delle opzioni di avviso... per specificare i dettagli di mittente/destinatario. For more information, refer to Configurazione delle opzioni di avviso (page 183).
Ignora opzioni generali di avviso e invia e-mail a	(Facoltativo) Invia un rapporto per posta elettronica a un indirizzo di posta specifico. Le opzioni di avviso di GFI LanGuard vengono ignorate.


New scheduled scan
Step 9 of 9: Review scheduled scan job
Please review the settings for this scheduled scan job.
Scheduled scan summary
Target
localhost
Triggering time
Occurs every day at 15:08:06.
Scanning profile
Full Scan
Credentials
GFI LanGuard 11 Attendant Service account
Auto-remediation
Automatically download and deploy missing patches and service packs, and uninstall unauthorized applications
Power Saving Options
Wait for offline computers and attempt to wake up offline computers.
Warning
Alerting options are not configured (email reports will not be sent).
Tell me more...
< Back
Finish
Cancel

Screenshot 42: Opzioni di creazione dei rapporti della scansione pianificata

12. Rivedere il riepilogo delle impostazioni di scansione e fare clic su **Fine**.

Nota

Tutte le nuove scansioni pianificate sono disabilitate per impostazione predefinita. Per abilitarle, selezionare la scheda **Configurazione>Scansioni pianificate** e fare clic sul pulsante .

Nota

Confermare che le nuove scansioni pianificate sono state impostate correttamente facendo clic sulla scheda **Monitor attività> Scansioni di sicurezza**. Le nuove scansioni pianificate sono elencate nella coda.

5.5.2 Modifica impostazioni scansione pianificata

Le pianificazioni di scansioni possono essere riviste, modificate o eliminate dalla scheda **Configurazione** > nodo **Scansioni pianificate**. Tutte le scansioni sono elencate nella pagina di riepilogo insieme alle informazioni rilevanti. Usare la barra degli strumenti scansione pianificata per eseguire le azioni descritte di seguito:

Table 36: Opzioni per la gestione dei profili di scansione

Opzioni	
	Aggiungi nuova scansione Visualizza la procedura guidata Nuova scansione pianificata e crea una nuova scansione pianificata.
	Elimina Usare questo pulsante per eliminare la scansione pianificata selezionata.
	Proprietà Rivede e modifica le proprietà della scansione selezionata.
	Abilita/disabilita Cambia lo stato della scansione selezionata in abilitato/disabilitato. In questo modo è possibile abilitare/sospendere la pianificazione di una scansione senza eliminare la scansione pianificata.
	Esegui scansione adesso Attiva la scansione pianificata selezionata. Questo pulsante ha la precedenza sulle impostazioni di data/ora della scansione pianificata ed esegue una scansione immediata.

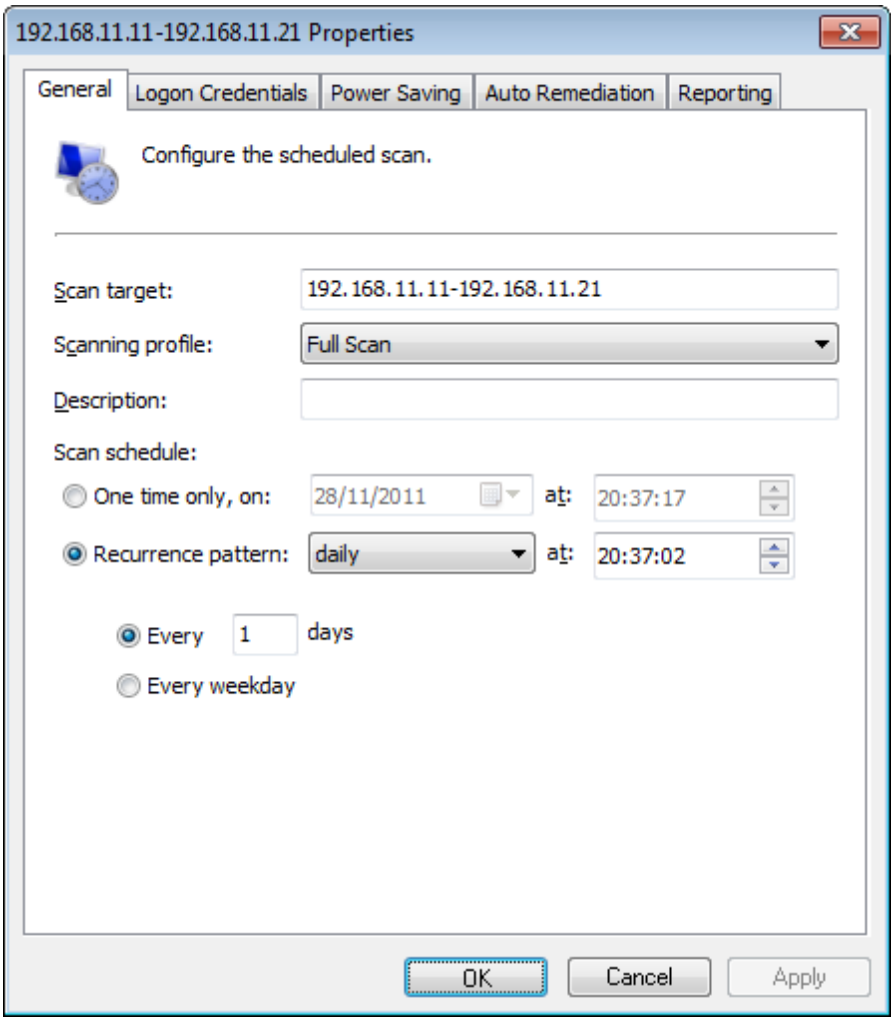
5.5.3 Configurazione proprietà scansione pianificata

La pagina delle proprietà della scansione pianificata consente di configurare tutti i parametri delle scansioni pianificate.

Per usare la scheda proprietà scansione pianificata:

1. Andare alla scheda **Configurazione** > **Scansioni pianificate**.

2. Selezionare la scansione pianificata e fare clic sul pulsante **Proprietà scansione pianificata**.



Screenshot 43: Proprietà scansione pianificata

Table 37: Proprietà scansione pianificata

Scheda	Descrizione
Generale	Apporta modifiche alle impostazioni di destinazione della scansione, al tipo di profilo di scansione e alla frequenza della scansione.
Credenziali di accesso	Specificare le credenziali di accesso utilizzate durante la scansione delle destinazioni specificate.
Risparmio energetico	Configurare le opzioni di risparmio energetico. Questa finestra di dialogo consente di configurare la scansione affinché attenda la connessione alla rete dei computer non in linea, tenti di attivare i computer non in linea e arresti i computer al termine della scansione.
Riparazione automatica	Configurare le opzioni di riparazione applicabili alla scansione attualmente configurata. Le opzioni comprendono il download e l'installazione delle patch e dei service pack mancanti e la disinstallazione di software non autorizzato.
Creazione di rapporti	Configurare le opzioni per la creazione di rapporti utilizzate per la scansione pianificata selezionata.

3. Fare clic su **OK**.

5.6 Scansioni pianificate agente

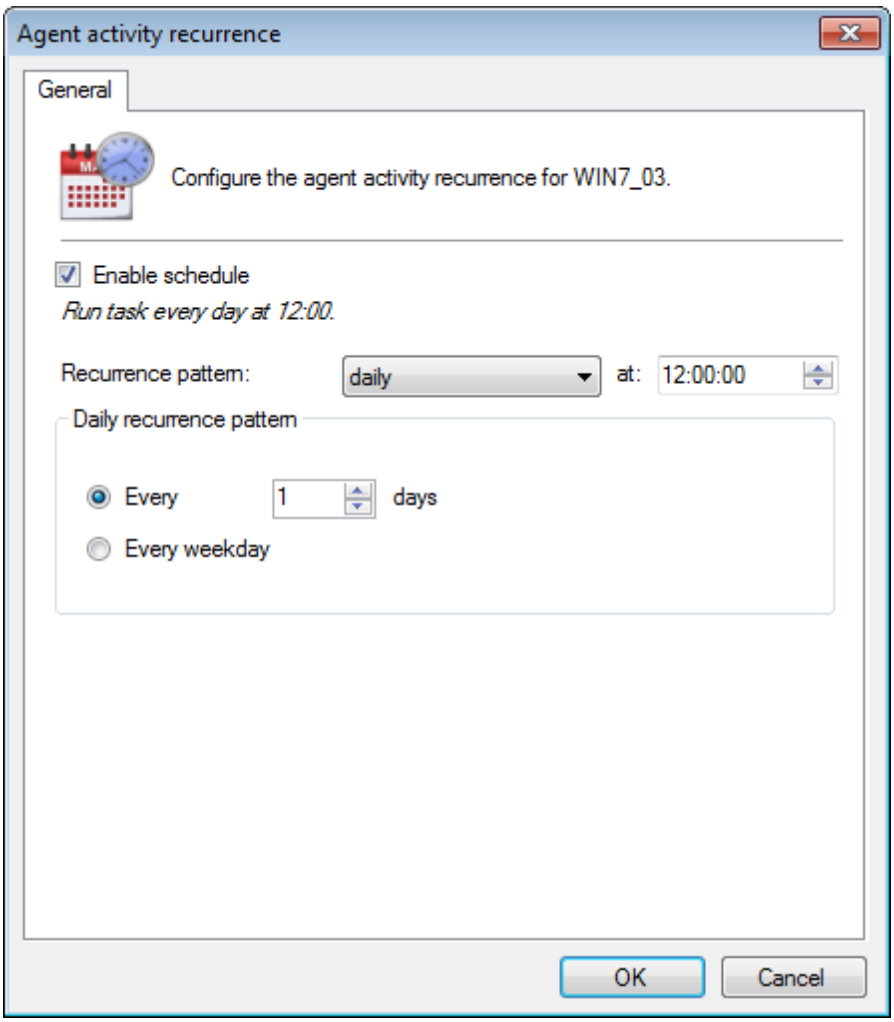
GFI LanGuard consente di configurare le scansioni pianificate sui computer che eseguono gli agenti. La pianificazione può essere configurata dalla finestra di dialogo Proprietà agente con la seguente procedura:

1. Avviare GFI LanGuard.

2. Dalla schermata **Home**, selezionare **Visualizza Dashboard**.

3. Dalla struttura computer fare clic con il pulsante destro del mouse sul computer/gruppo di computer che si desidera configurare, quindi selezionare **Proprietà**.

4. Fare clic sulla scheda **Stato agente > Modifica pianificazione scansione...**.



Screenshot 44: Ricorrenza attività agente

5. Selezionare **Abilita pianificazione** e configurare lo schema di ricorrenza.

6. Fare clic su **OK**.

Nota

Le proprietà aggiuntive possono essere configurate dalla finestra di dialogo **Proprietà**. For more information, refer to Proprietà agente (page 49).

5.6.1 Avvio di una scansione agente manuale

Per avviare una scansione su richiesta sul computer dell'agente:

1. Avviare GFI LanGuard.
2. Fare clic su **Visualizza dashboard** e selezionare i computer che si desidera sottoporre a scansione.
3. Dalla sezione **Stato agente** fare clic su **Esegui scansione adesso**.

> **Nota**
>
> **Esegui scansione adesso** è visibile solo quando **Stato agente** corrisponde a **Agente installato**.

6 Dashboard

La sezione **Dashboard** fornisce informazioni di sicurezza complete basate sui dati acquisiti durante le scansioni. La sezione Dashboard consente inoltre di individuare il livello attuale di vulnerabilità della rete, i computer più vulnerabili e il numero di computer nel database.

Argomenti del presente capitolo:

6.1 Ottenimento dei risultati dal dashboard 85
6.2 Utilizzo del Dashboard 86
6.3 Utilizzo della struttura computer 86
6.4 Utilizzo attributi 90
6.5 Azioni Dashboard 92
6.6 Esportazione elenco problemi 93
6.7 Visualizzazioni Dashboard 93

6.1 Ottenimento dei risultati dal dashboard

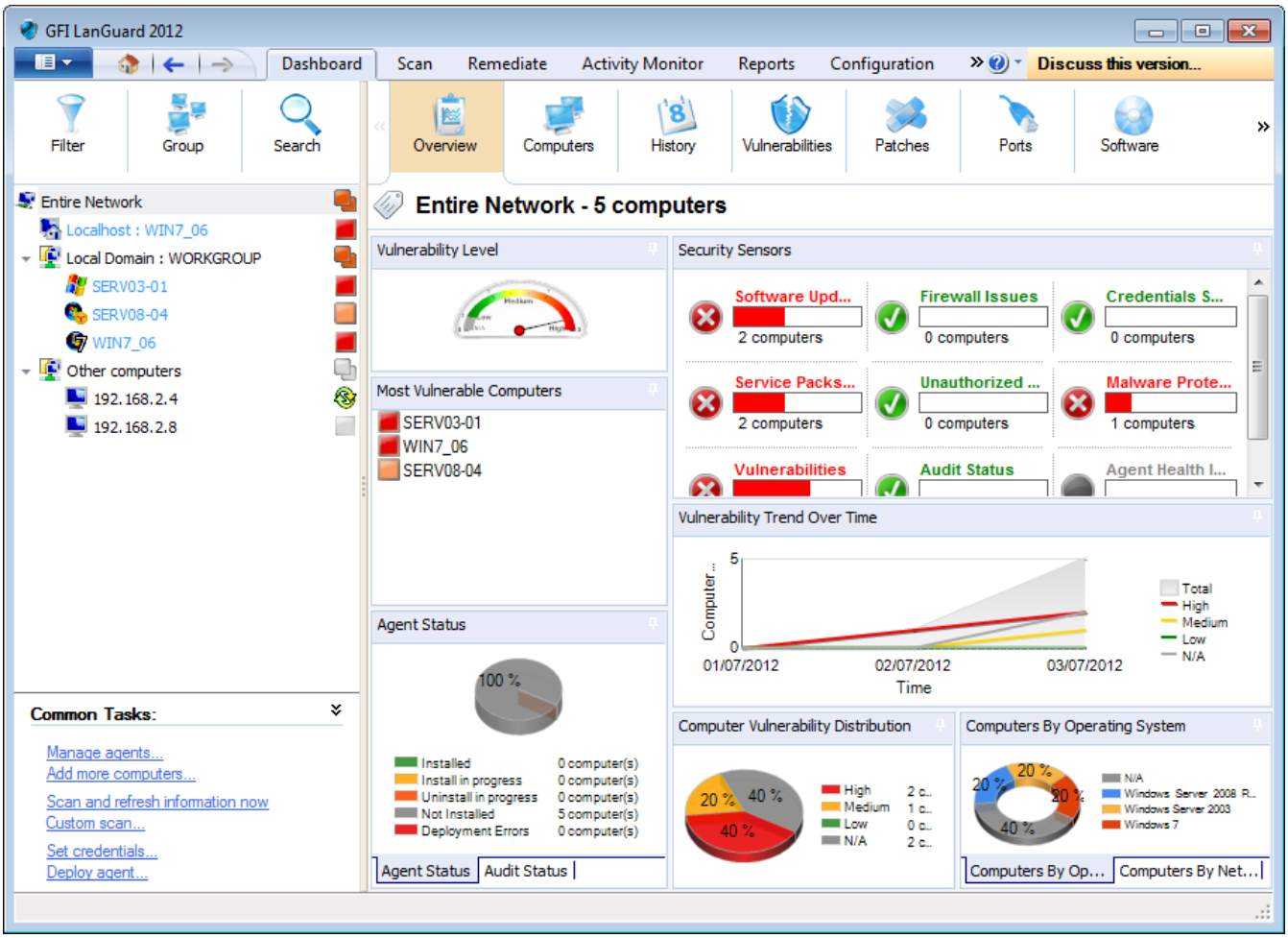
Il dashboard è una funzionalità importante di GFI LanGuard. Come punto centrale dell'applicazione, consente l'esecuzione di tutte le attività comuni supportate da GFI LanGuard, tra cui:

- monitoraggio di tutti i computer gestiti da GFI LanGuard;
- gestione delle destinazioni di scansione; aggiunta, modifica o rimozione di computer, domini e gruppi di lavoro;
- distribuzione di agenti nei computer di destinazione e configurazione delle impostazioni agente;
- Configurazione delle credenziali del computer
- Configurazione delle opzioni di riparazione automatica
- Configurazione dell'individuazione di rete ricorrente nei domini gestiti/gruppi di lavoro/unità organizzative
- Attivazione di scansioni di protezione/aggiornamento informazioni di scansione
- analisi dello stato di sicurezza dei computer e controllo dei dettagli.
- Passaggio alle posizioni pertinenti tramite selezione dei sensori di protezione e dei grafici.

6.2 Utilizzo del Dashboard

Questa sezione fornisce le informazioni necessarie su come utilizzare il Dashboard di GFI LanGuard. Per visualizzare il **Dashboard**:

1. Avviare GFI LanGuard e fare clic sulla scheda **Dashboard**.



Screenshot 45: Visualizza dashboard

2. Dall'elenco computer selezionare un computer o un gruppo di computer. Le informazioni del dashboard vengono aggiornate in base alla selezione effettuata.

6.3 Utilizzo della struttura computer

GFI LanGuard include opzioni di filtro e raggruppamento che consentono l'individuazione rapida di un computer o dominio e la visualizzazione immediata dei risultati.

Una volta selezionato un computer o un gruppo dalla struttura computer, i risultati vengono aggiornati automaticamente nel dashboard. Premere **CTRL** e selezionare più computer per visualizzare i risultati di computer specifici.

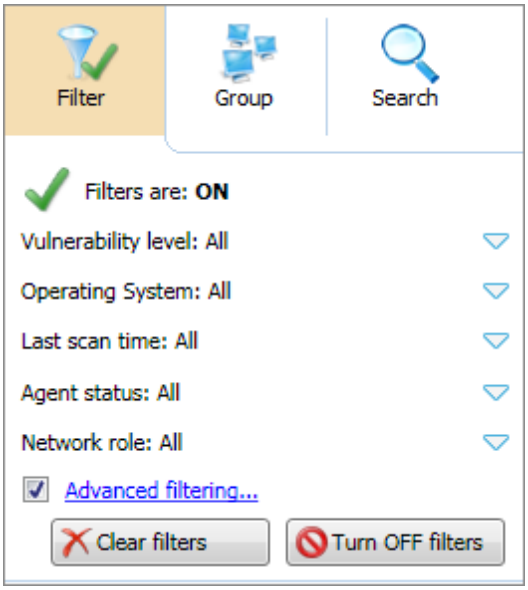
Seguono le funzioni supportate dalla struttura di computer:

- Filtro semplice
- Filtro avanzato
- Raggruppamento
- Ricerca

6.3.1 Filtro semplice

Per filtrare in base a un computer o gruppo specifici:

1. Dal riquadro di sinistra selezionare **Filtro**.
2. Configurare i criteri, quindi fare clic su **Attiva filtri**.

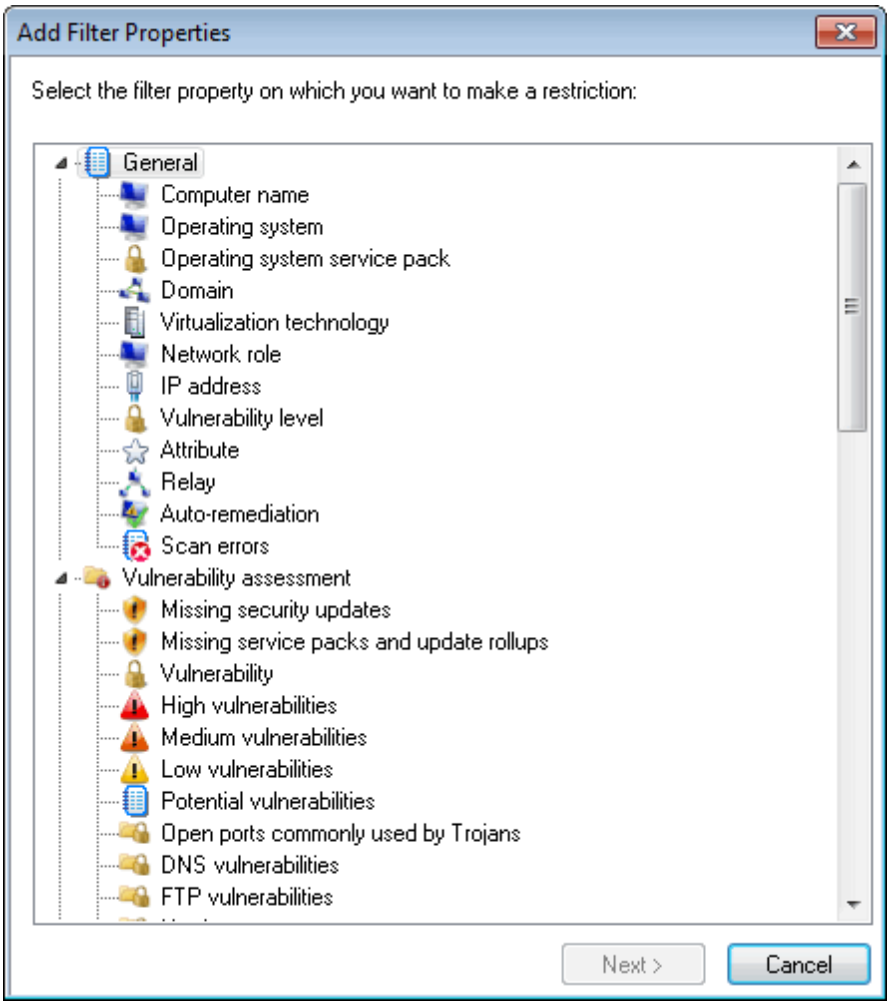


Screenshot 46: Filtro semplice

6.3.2 Filtro avanzato

Per filtrare in base a un computer o un gruppo con il filtro avanzato:

1. Dal riquadro di sinistra fare clic su **Filtro** e su **Filtro avanzato...**
2. Dalla finestra di dialogo **Filtro avanzato**, fare clic su **Aggiungi**.



Screenshot 47: Aggiungi proprietà filtro

3. Selezionare la proprietà filtro da limitare, quindi fare clic su **Avanti**.

4. Selezionare la condizione e immettere il valore della condizione. Fare clic su **Aggiungi**.

5. Ripetere i passaggi da 2 a 4 per ciascuna condizione. Fare clic su **OK**.

6.3.3 Raggruppamento

Per raggruppare i computer in base ad attributi specifici:

1. Dal pannello di sinistra, selezionare **Gruppo**.

2. Selezionare uno dei seguenti attributi:

- Dominio e unità organizzativa
- Sistema operativo
- Ruolo di rete
- Distribuzione relay
- Attributi.

Nota

Se è selezionato **Attributi**, selezionare l'attributo dall'elenco a discesa. For more information, refer to Utilizzo attributi (page 90).

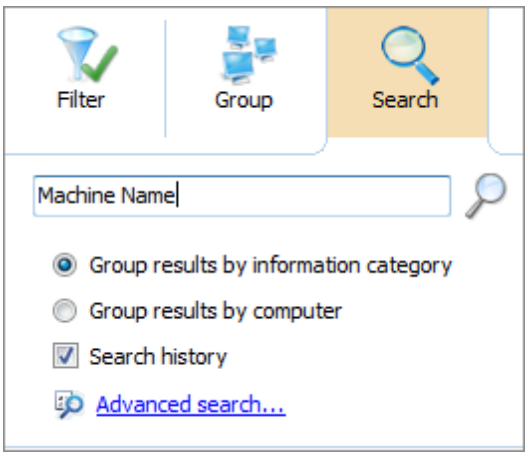
3. Se è selezionato Attributi, selezionare l'attributo dall'elenco a discesa.

4. Fare clic su **Applica raggruppamento**.

6.3.4 Ricerca

La scheda Cerca all'interno della **struttura computer** consente di effettuare la ricerca e visualizzare i risultati per un computer o gruppo specifici. Per visualizzare i risultati per un computer specifico:

1. Dalla **struttura computer**, selezionare **Cerca**.



Screenshot 48: Ricerca di computer e gruppi specifici

2. Digitare i criteri di ricerca e utilizzare le seguenti opzioni:

Table 38: Opzioni di ricerca

Opzione	Descrizione
Raggruppa risultati per categoria di informazioni	I risultati di ricerca sono raggruppati per categoria. Il risultato contiene le informazioni del computer più aggiornate. Inoltre, i risultati di ricerca sono raggruppati per: » Informazioni computer » Dispositivi hardware » Utenti connessi » Processi » Tecnologia virtuale
Raggruppa risultati per computer	Risultati di ricerca raggruppati in base al nome del computer. Il risultato contiene le informazioni del computer più aggiornate.
Ricerca nella cronologia	I risultati di ricerca includono le informazioni di scansioni precedenti.
Ricerca avanzata	Configurare le opzioni di ricerca avanzate. **Nota** For more information, refer to Ricerca nel testo completo (page 180).

6.4 Utilizzo attributi

Gli attributi consentono il raggruppamento e la configurazione di computer singoli o multipli in un'unica operazione. Gli attributi consentono inoltre la riparazione di vulnerabilità o la distribuzione di software su computer specifici sulla base dell'attributo assegnato. Le seguenti sezioni contengono informazioni relative a:

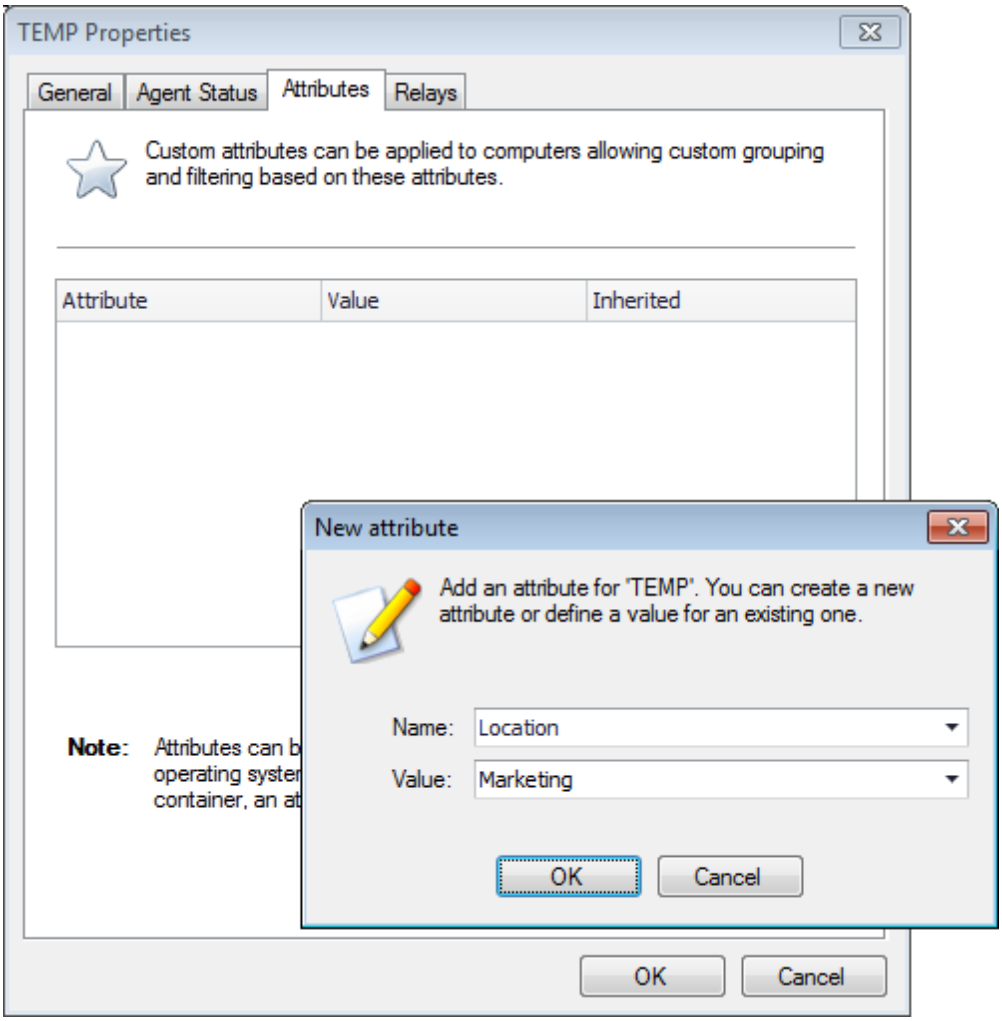
- Assegnazione attributi a un computer
- Assegnazione attributi a un gruppo
- Configurazione attributi

6.4.1 Assegnazione attributi a un computer

Per assegnare gli attributi a un singolo computer:

1. Fare clic sulla scheda **Dashboard**.

2. Dalla struttura computer fare clic con il pulsante destro del mouse su un computer e selezionare **Assegna attributi**.



Screenshot 49: Assegnazione attributi: Computer singolo

3. Dalla finestra di dialogo **Proprietà**, scheda **>Attributi**, fare clic su **Aggiungi**.

4. Configurare le impostazioni dei nuovi attributi, quindi fare clic su **OK**.

5. Fare clic su **OK** per salvare le impostazioni selezionate.

6.4.2 Assegnazione attributi a un gruppo

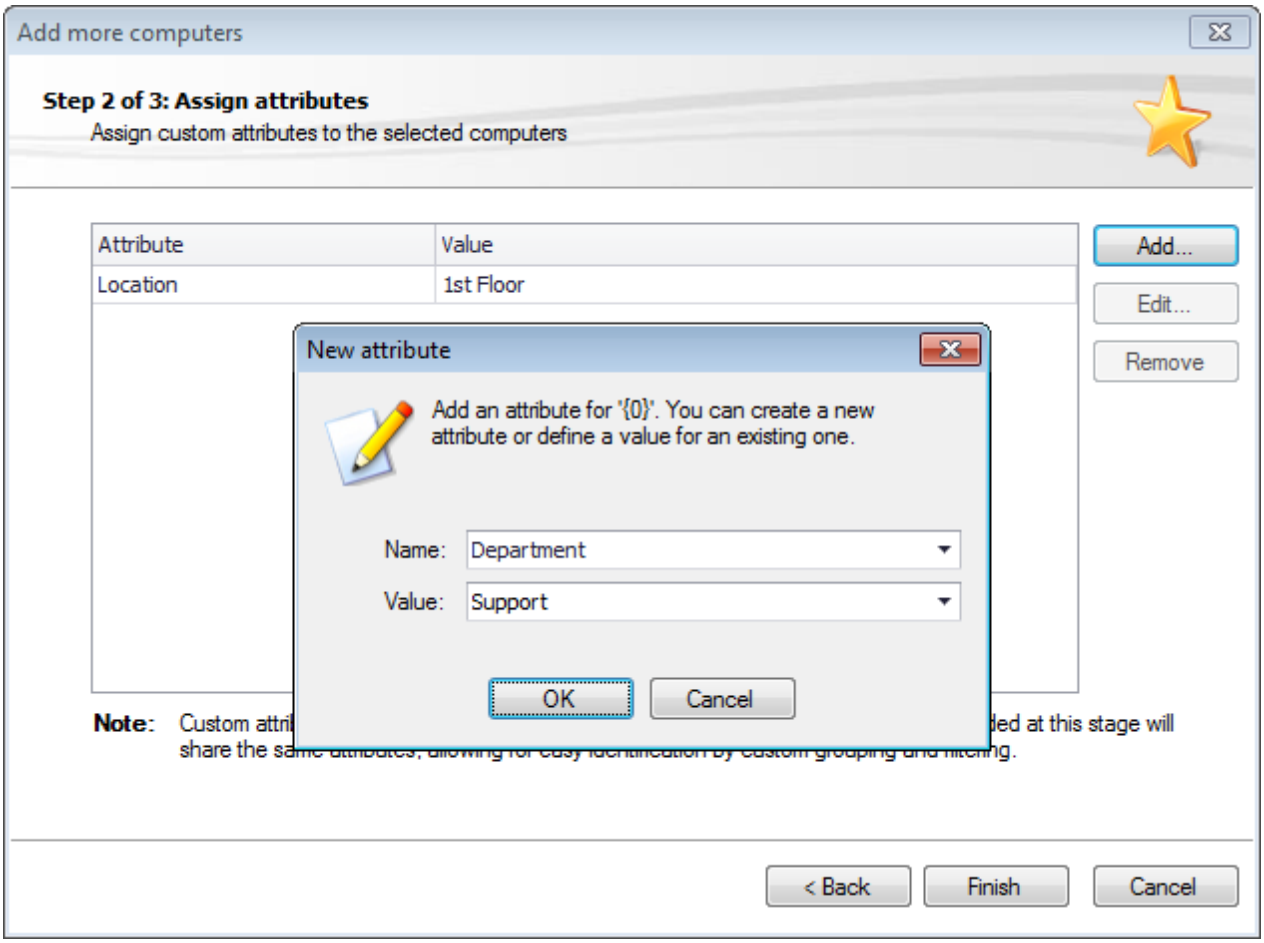
GFI LanGuard consente di assegnare attributi a specifici gruppi, domini, unità organizzative e reti. Una volta assegnati gli attributi, ciascun membro del gruppo selezionato eredita le impostazioni degli attributi.

Per assegnare gli attributi a un gruppo:

1. Fare clic sulla scheda **Dashboard**.

2. Dall'elenco dei computer, fare clic con il pulsante destro del mouse sulla rete e selezionare **Assegna attributi**.

3. Dalla procedura guidata **Aggiungi altri computer**, selezionare la rete, quindi fare clic su **Avanti**.



Screenshot 50: Assegnazione attributi: Più computer

4. Fare clic su **Aggiungi** e configurare i rispettivi attributi. Per modificare o rimuovere gli attributi selezionati, utilizzare i pulsanti **Modifica** e **Rimuovi**.

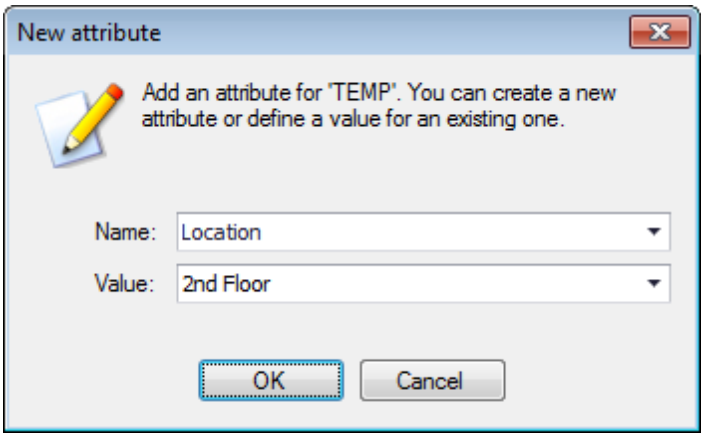
5. Per salvare le impostazioni, fare clic su **Fine**.

6.4.3 Configurazione attributi

Per configurare gli attributi:

1. Dalla finestra di dialogo **Proprietà**, fare clic sulla scheda **Attributi**.

2. Per avviare la finestra di dialogo **Nuovo attributo**, fare clic su **Aggiungi**.



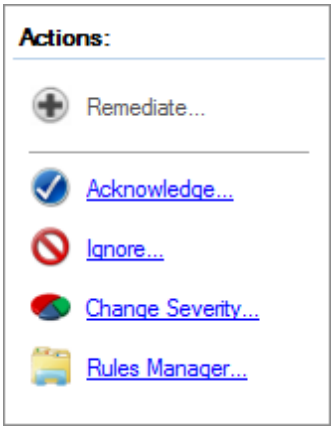
Screenshot 51: Finestra di dialogo Nuovo attributo

3. Dal menu a discesa **Nome**, selezionare un attributo o immettere un nome per crearne uno nuovo.
4. Nel campo **Valore**, specificare un valore per l'attributo. Fare clic su **OK**.
5. Ripetere i passaggi da 2 a 4 fino all'aggiunta di tutti gli attributi richiesti.
6. Fare clic su **OK** per salvare le impostazioni selezionate.

6.5 Azioni Dashboard

La sezione **Azioni** consente di gestire e riparare le vulnerabilità e le patch mancanti rilevate nella rete. Per accedere alla sezione **Azioni**:

1. Selezionare la scheda **Dashboard**.
2. Fare clic sulla scheda **Vulnerabilità** o **Patch**.



Screenshot 52: Sezione Azioni del Dashboard

3. Selezionare una delle seguenti azioni:

Table 39: Azioni Dashboard

Azione	Descrizione
Riparazione	Per distribuire e gestire le patch mancanti, avviare il Centro riparazioni. **Nota** For more information, refer to Riparazione manuale (page 143).
Riconosci	Avviare la finestra di dialogo Regola - Riconosci patch. Consente di riconoscere i problemi affinché non interessino il livello di vulnerabilità della rete. Configurare il computer a cui si applica questa regola

Azione	Descrizione
Ignora	Avviare la finestra di dialogo Regola-Ignora patch. Consente di ignorare le patch mancanti o le vulnerabilità, affinché non vengano segnalate come errori in futuro. Configurare i computer a cui si applica questa regola e l'intervallo di tempo in cui il problema verrà ignorato.
Modifica gravità	Avviare la finestra di dialogo Regola-Modifica gravità. Ciò consente di modificare il livello di gravità di una vulnerabilità. Configurare i computer a cui si applica questa regola e il livello di gravità.
Gestione regole	Avviare la finestra di dialogo Gestione regole. Ciò consente di cercare e rimuovere le regole configurate.

6.6 Esportazione elenco problemi

GFI LanGuard consente di esportare gli elenchi dei problemi in Portable Document Format (PDF), Microsoft Office Excel (XLS) o Hyper Text Markup Language (HTML). Quando un elenco supporta l'esportazione, queste icone vengono visualizzate nell'angolo superiore destro dell'elenco. Selezionare l'icona rispettiva e configurare le impostazioni di esportazione.

6.7 Visualizzazioni Dashboard

Il dashboard di GFI LanGuard è costituito da visualizzazioni multiple. Esse consentono un monitoraggio in tempo reale delle destinazioni di scansione e permettono di eseguire operazioni di segnalazione e riparazione istantanee. Le seguenti sezioni contengono informazioni relative a:

- Panoramica Dashboard
- Visualizzazione Computer
- Visualizzazione Cronologia
- Visualizzazione vulnerabilità
- Visualizzazione Patch
- Visualizzazione Porte
- Visualizzazione Software
- Visualizzazione Hardware
- Visualizzazione Informazioni di sistema

6.7.1 Panoramica

Screenshot 53: Panoramica Dashboard

La **panoramica Dashboard** è una rappresentazione grafica del livello di sicurezza/vulnerabilità di un computer singolo, dominio o dell'intera rete.

Una volta selezionato un computer o dominio, i risultati relativi al computer/dominio selezionato vengono aggiornati automaticamente nel dashboard. Segue una descrizione di ciascuna sezione presente nel dashboard:

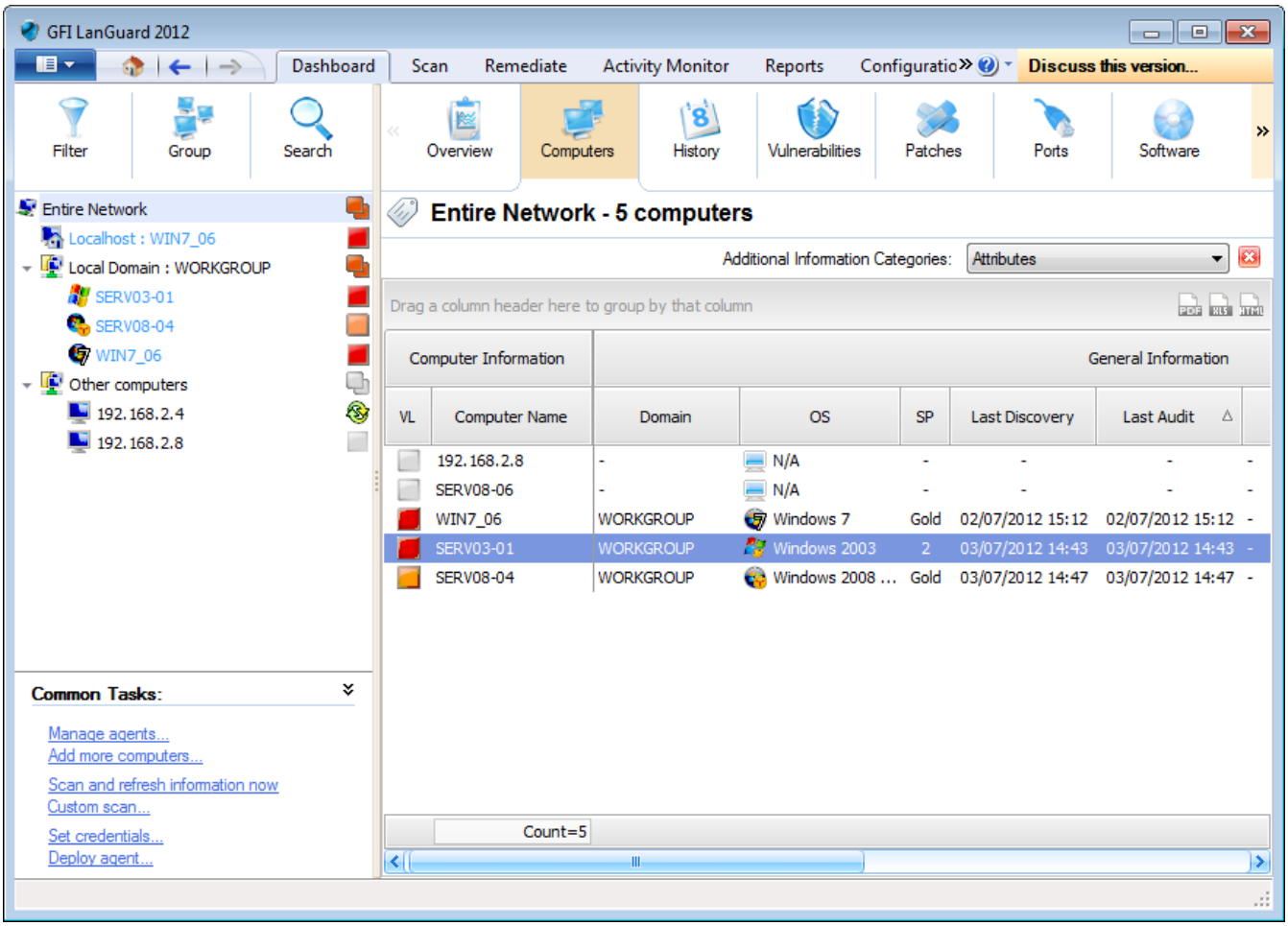
Table 40: Informazioni software dal controllo

Sezione	Descrizione
Livello di sicurezza di rete	Questa valutazione indica il livello di vulnerabilità di un computer/una rete, in base al numero e al tipo di vulnerabilità e/o patch mancanti trovate. Un livello di vulnerabilità elevato è il risultato di vulnerabilità e/o patch mancanti la cui gravità media viene classificata come elevata.
Distribuzione vulnerabilità del computer	Questo grafico è disponibile solo quando si seleziona un dominio o gruppo di lavoro e visualizza la distribuzione delle vulnerabilità nella rete. Questo grafico individua quanti computer hanno una valutazione di vulnerabilità elevata, media e bassa.
Computer più vulnerabili	Questo elenco è disponibile quando si seleziona un dominio o gruppo di lavoro e visualizza i computer più vulnerabili rilevati durante la scansione. Il colore dell'icona a sinistra indica il livello di vulnerabilità.

Sezione	Descrizione
Stato agente	Quando si seleziona un dominio o gruppo di lavoro, viene visualizzato un grafico che riporta lo stato generale dell'agente di tutti i computer all'interno del dominio/gruppo di lavoro. Ciò consente di individuare il numero di agenti installati o con installazione in sospeso nel dominio/gruppo di lavoro selezionato. Quando si seleziona un computer singolo, questa sezione visualizza un'icona che rappresenta lo stato dell'agente. Le icone sono descritte di seguito: » **Non installato**: l'agente non è installato sul computer di destinazione. » **Installazione in sospeso**: l'installazione è in sospeso. Uno stato può essere in sospeso quando il computer non è in linea o l'agente è in fase di installazione. » **Disinstallazione in sospeso**: la disinstallazione è in sospeso. Uno stato può essere in sospeso quando il computer non è in linea o l'agente è in fase di disinstallazione. » **Installato**: l'agente è installato sul computer di destinazione. » **Agente relay installato:** i computer selezionati sono agenti relay.
Stato controllo	Questo grafico è disponibile solo quando si seleziona un dominio o gruppo di lavoro e consente di identificare quanti controlli sono stati eseguiti sulla rete, suddivisi in gruppi temporali.
Tendenze della vulnerabilità nel tempo	Quando si seleziona un dominio o gruppo di lavoro, questa sezione visualizza un grafico a linee che indica la modifica del livello di vulnerabilità nel tempo, raggruppato per numero di computer. Quando si seleziona un computer singolo, questa sezione visualizza un grafico che indica il cambiamento del livello di vulnerabilità nel tempo per il computer selezionato.
Computer in base al ruolo di rete	Questo grafico è disponibile solo quando si seleziona un dominio o gruppo di lavoro e visualizza il numero di computer sottoposti a controllo, raggruppati in base al ruolo di rete. Tra gli altri ruoli, questo grafico identifica il numero di server e workstation per il dominio selezionato.
Computer in base al sistema operativo	Questo grafico è disponibile solo quando si seleziona un dominio o gruppo di lavoro e visualizza il numero di computer sottoposti a controllo, raggruppati in base al sistema operativo installato.
Dettagli computer	Questa sezione è disponibile quando si seleziona un computer singolo e consente di visualizzare i dettagli del computer selezionato.
Attività di scansione	Questo grafico a linee è disponibile solo quando si sceglie un computer singolo e consente di visualizzare il numero di scansioni/controlli eseguiti sul computer selezionato. Inoltre, consente di controllare che le scansioni pianificate siano effettuate.
Attività di riparazione	Questo grafico a linee è disponibile solo quando si sceglie un computer singolo e consente di visualizzare il numero di attività di riparazione eseguite sul computer selezionato. Inoltre, consente di verificare che sia eseguita la riparazione automatica.
Primi 5 problemi da risolvere	Questa sezione è disponibile solo quando si seleziona un computer singolo e visualizza i primi cinque problemi da risolvere per il computer selezionato.
Statistiche risultati	Questa sezione è disponibile solo quando si seleziona un computer singolo e visualizza una panoramica dei risultati del controllo. Inoltre, il risultato consente di identificare il numero di patch mancanti, di applicazioni installate, di porte aperte e di servizi in esecuzione.

Sezione	Descrizione
Sensori di protezione	Questa sezione consente un'identificazione immediata dei problemi. Fare clic su un sensore per esplorare e visualizzare i problemi e le vulnerabilità per un computer o gruppo specifico. I sensori consentono di identificare: » Aggiornamenti software mancanti » Service pack mancanti » Vulnerabilità » Problemi firewall » Applicazioni non autorizzate » Stato controllo » Impostazione credenziali » Problemi protezione antimalware » Problemi integrità agente.

6.7.2 Visualizzazione Computer



Screenshot 54: Analisi risultati per computer

Per raggruppare i risultati di controllo in base al computer, selezionare questa visualizzazione. Dall'elenco a discesa, selezionare una delle opzioni descritte di seguito:

Table 41: Visualizzazione in base alle informazioni dei computer

Opzione	Descrizione
Dettagli agente	Per visualizzare lo stato dell'agente, selezionare questa opzione. Questa opzione consente di identificare se un agente è installato in un computer e in tal caso, visualizza il tipo di credenziali utilizzate dall'agente.
Vulnerabilità	Visualizzazione del numero di vulnerabilità rilevate nel computer raggruppate per gravità. Il livello di gravità di una vulnerabilità può essere: » Alto » Medio » Basso » Potenziale
Stato dell'applicazione di patch	Visualizzazione del numero di: » Aggiornamenti di sicurezza/non di sicurezza mancanti » Service pack e aggiornamenti cumulativi mancanti » Aggiornamenti di sicurezza/non di sicurezza installati » Service pack e aggiornamenti cumulativi installati.

Opzione	Descrizione
Porte aperte	Visualizzazione del numero di: » Porte TCP aperte » Porte UDP aperte » Backdoor
Software	Visualizzazione del numero di: » Motori antiphishing » Motori antispyware » Motori antivirus » Applicazioni di backup » Applicazioni di prevenzione perdita di dati » Applicazioni di accesso a periferiche e di crittografia disco » Firewall » Applicazioni installate » Messenger istantanei » Applicazioni peer to peer » Applicazioni non autorizzate » Macchine virtuali » Client VPN » Browser web
Hardware	Visualizzazione di informazioni relative a: » Numero di unità disco » Spazio libero su disco » Dimensioni memoria » Numero di processori » Altro hardware.
Informazioni di sistema	Visualizzazione di informazioni relative a: » Numero di cartelle condivise » Numero di gruppi » Numero di utenti » Utenti registrati » Stato criterio di controllo
Attributi	Aggiunge una colonna **Attributi** e raggruppa le destinazioni di scansione in base all'attributo assegnato.

Nota

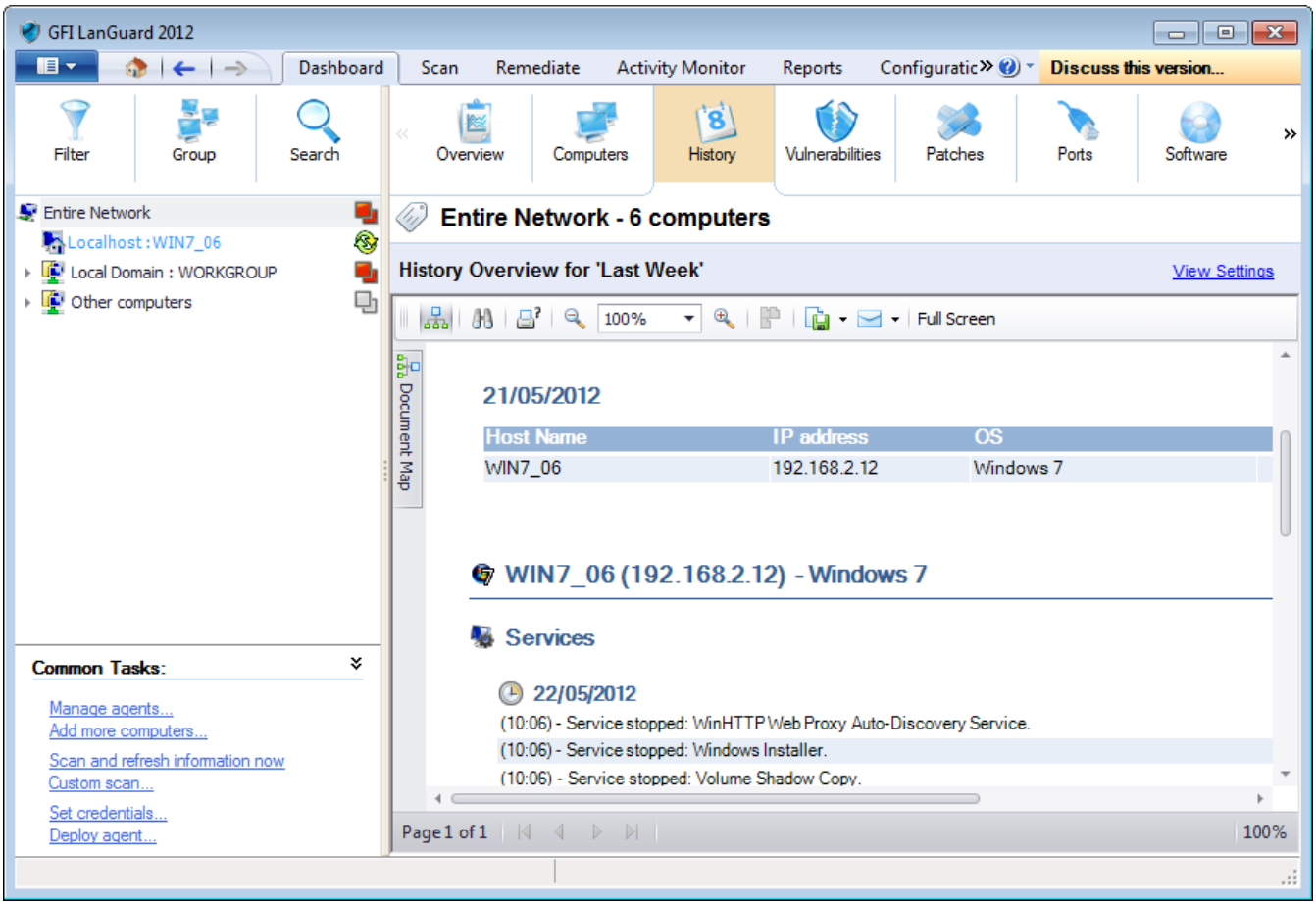
Per aprire la scheda **Panoramica** e visualizzare maggiori dettagli su un computer specifico, fare doppio clic su un computer dall'elenco.

Nota

Per raggruppare i dati in base a criteri, trascinare l'intestazione di una colonna nell'area designata.

6.7.3 Visualizzazione Cronologia

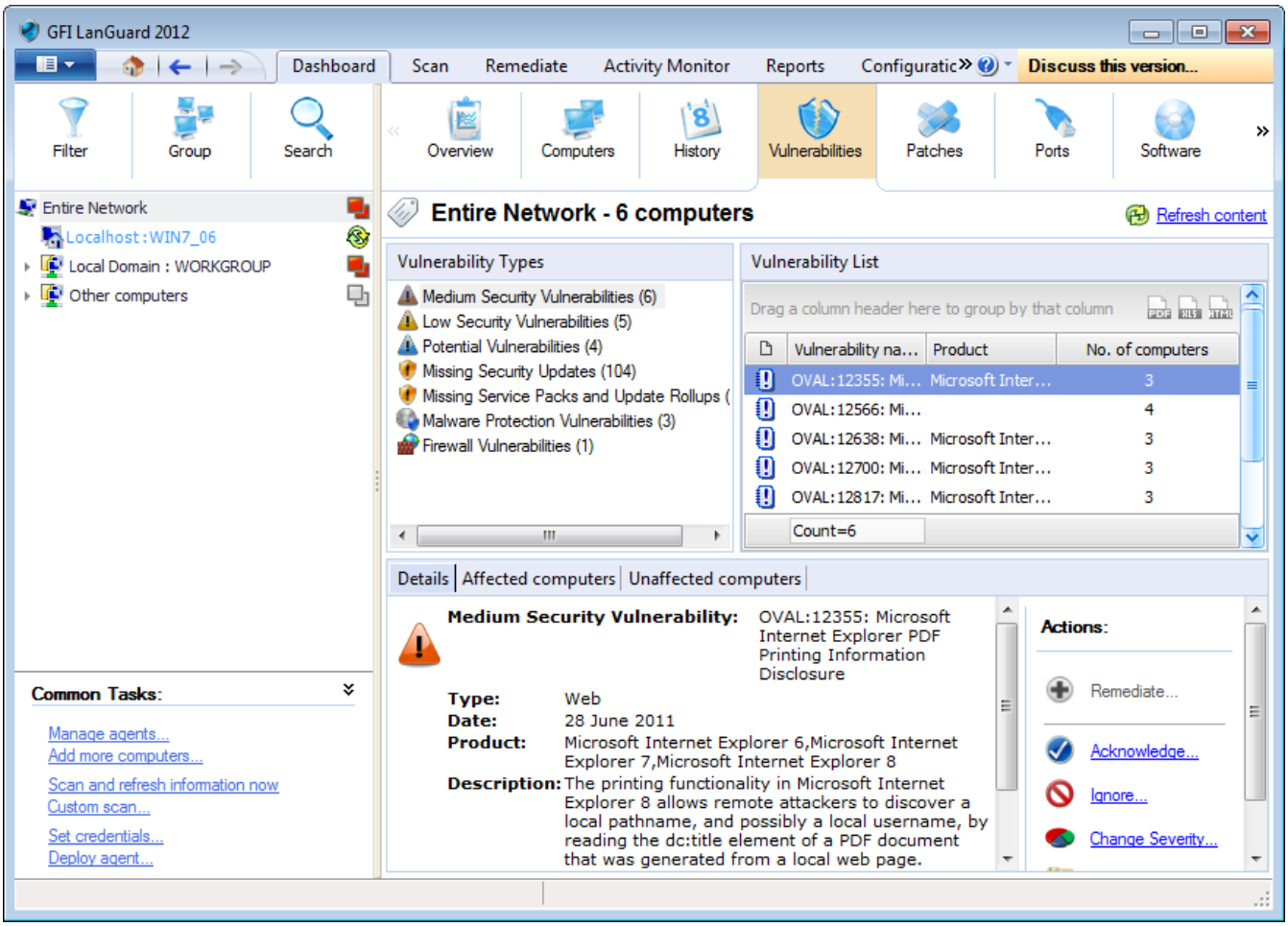
Per raggruppare i risultati di controllo in base alla data per un computer specifico, selezionare questa visualizzazione. Per configurare la data di inizio della cronologia o il periodo della cronologia, fare clic sul collegamento fornito.



Screenshot 55: Visualizzazione Cronologia nel Dashboard

6.7.4 Visualizzazione vulnerabilità

Visualizzazione di più dettagli sulle vulnerabilità rilevate nella rete e sul numero di computer interessati. Quando una vulnerabilità è selezionata dall'**Elenco vulnerabilità**, la sezione **Dettagli** fornisce ulteriori informazioni sulla vulnerabilità selezionata. Dalla sezione **Dettagli**, fare clic su **Computer interessati** o **Computer non interessati**, per visualizzare un elenco di computer interessati e non.

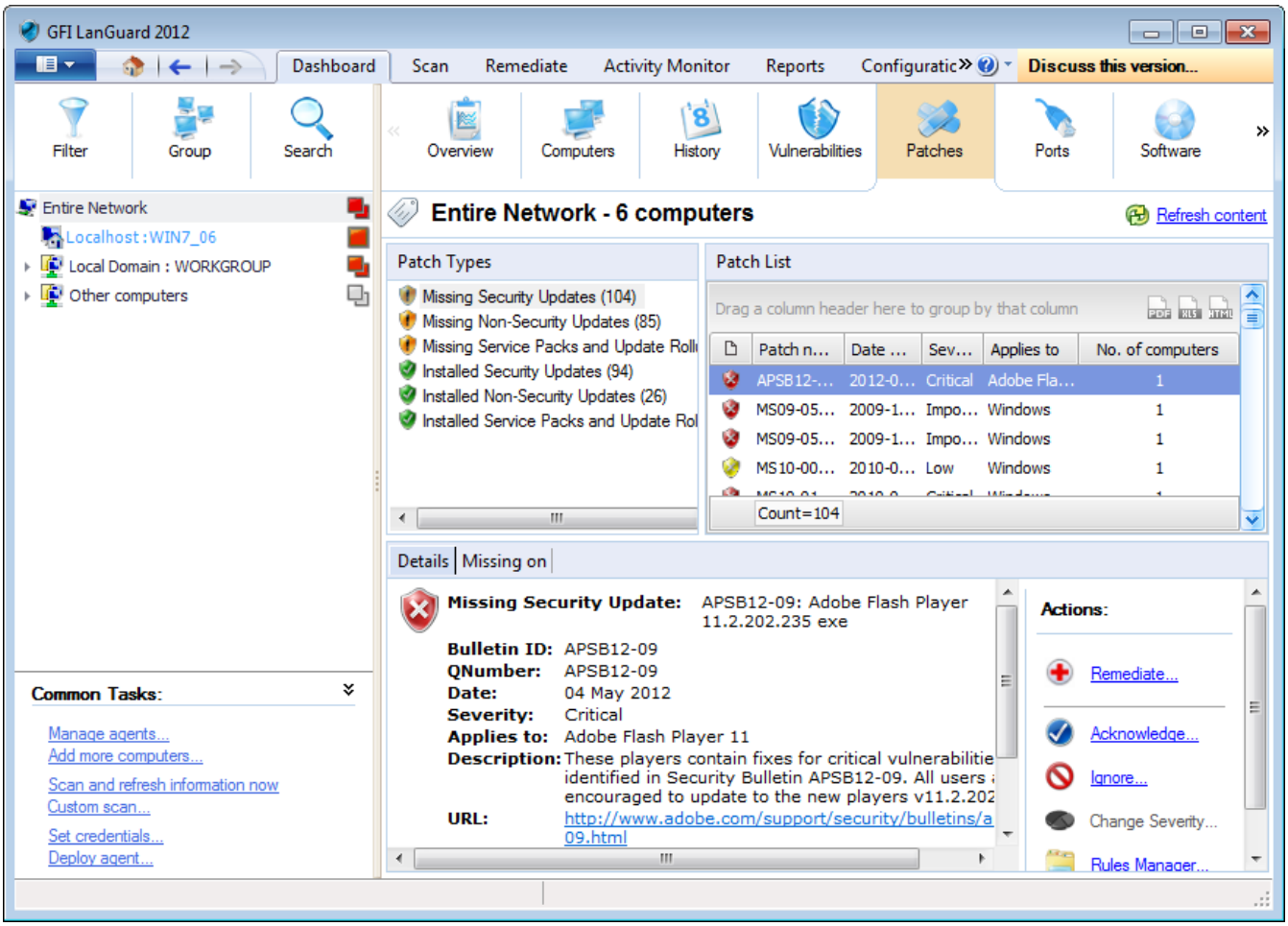


Screenshot 56: Visualizzazione Vulnerabilità nel Dashboard

> **Nota**
>
> Per raggruppare i dati in base a criteri, trascinare l'intestazione di una colonna nell'area designata.

6.7.5 Visualizzazione Patch

Visualizzazione di più dettagli sulle patch installate/mancanti e sui service pack individuati durante un controllo di rete. Quando una patch/service pack è selezionato dall'Elenco, la sezione **Dettagli** fornisce ulteriori informazioni sulla patch/service pack selezionato. Dalla sezione **Dettagli**, fare clic su **Mancante in** per visualizzare un elenco di computer dove manca la patch selezionata.

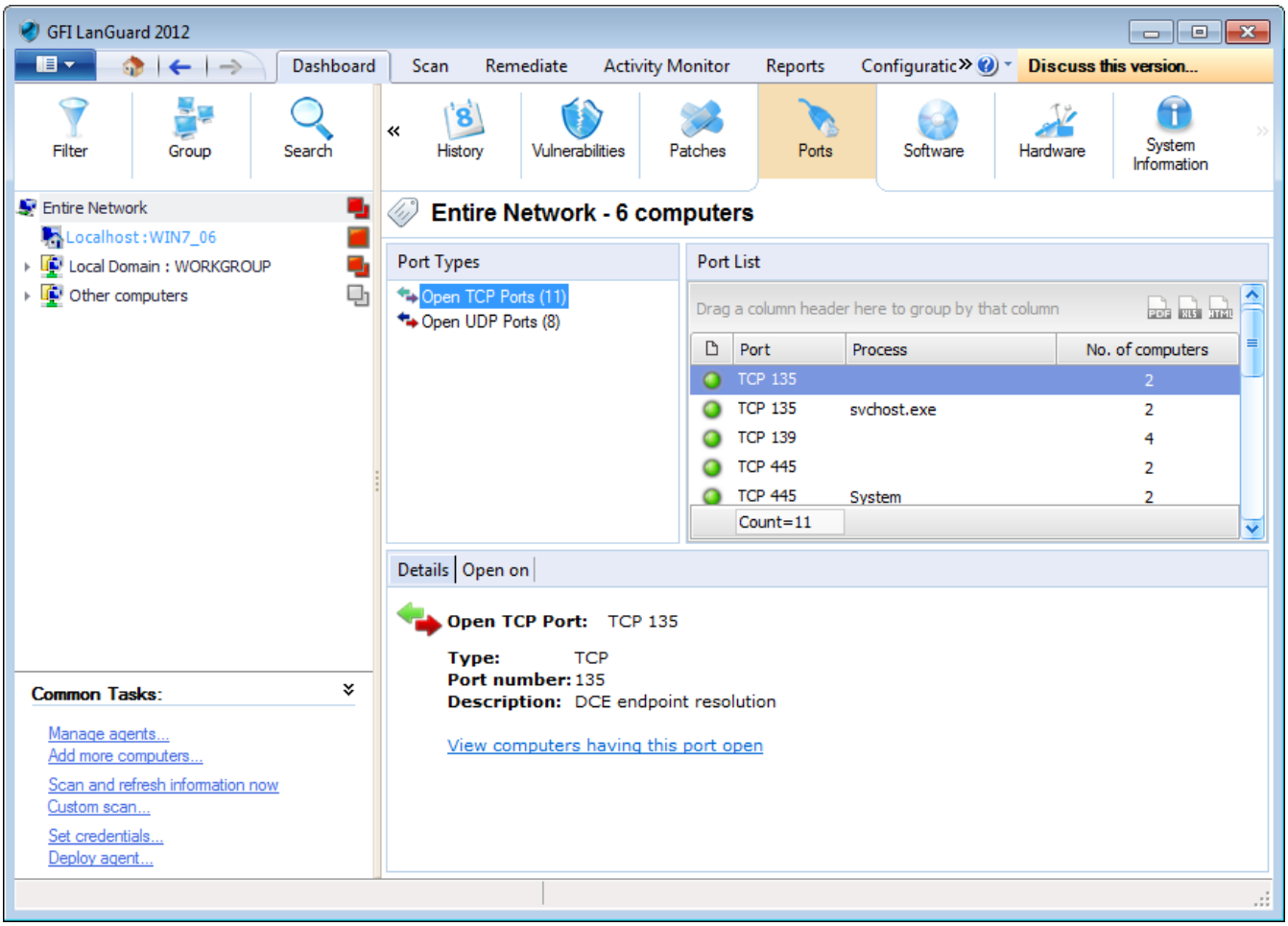


Screenshot 57: Visualizzazione Patch nel Dashboard

> **Nota**
>
> Per raggruppare i dati in base a criteri, trascinare l'intestazione di una colonna nell'area designata.

6.7.6 Visualizzazione Porte

Visualizzazione di maggiori dettagli sulle porte aperte rilevate durante un controllo di rete. Quando una porta è selezionata da **Elenco porte**, la sezione **Dettagli** fornisce maggiori informazioni sulla porta selezionata. Dalla sezione **Dettagli**, selezionare **Visualizza computer con questa porta aperta** per visualizzare un elenco di computer con la porta aperta.



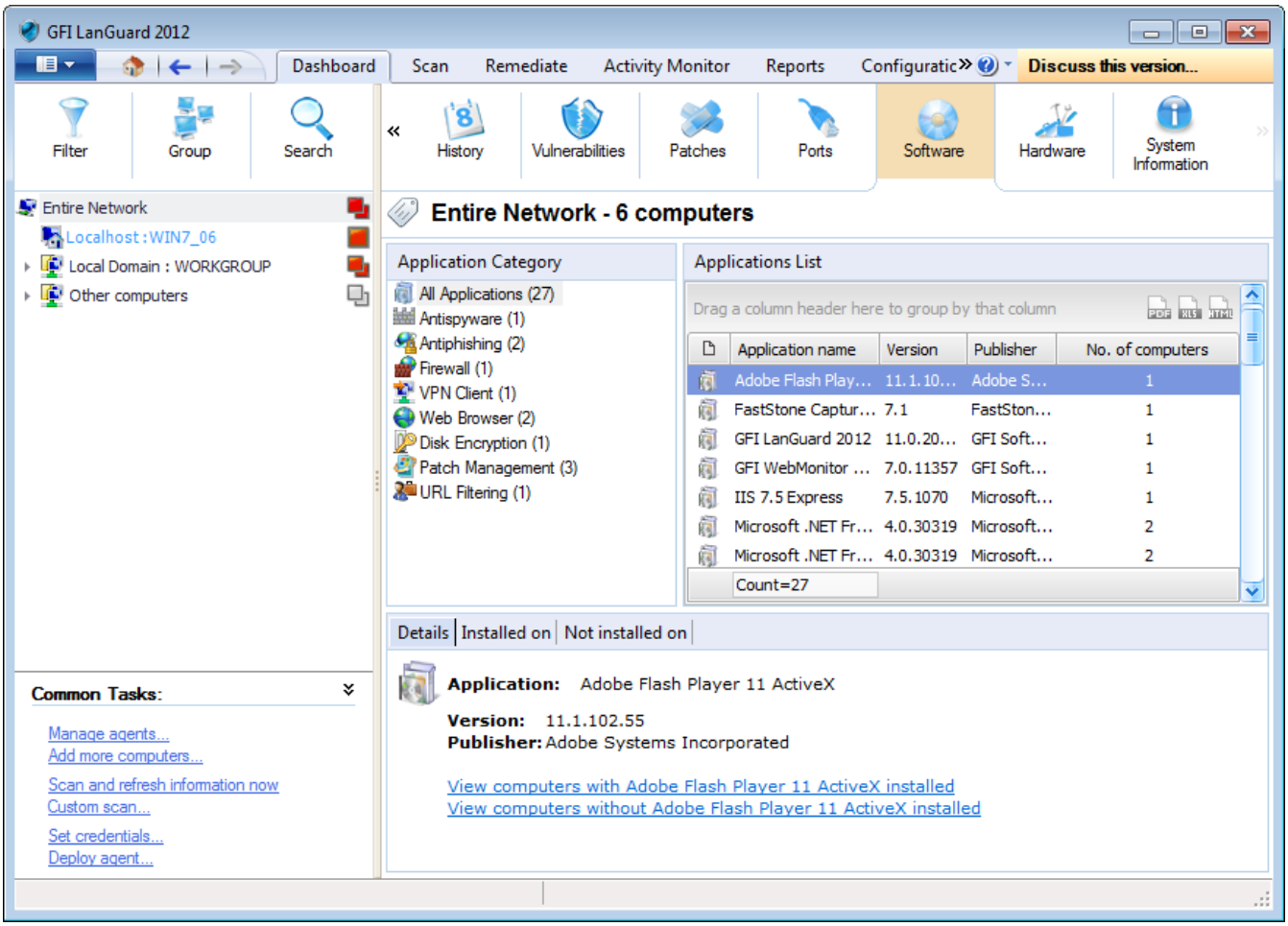
Screenshot 58: Visualizzazione Porte nel Dashboard

Nota

Per raggruppare i dati in base a criteri, trascinare l'intestazione di una colonna nell'area designata.

6.7.7 Visualizzazione Software

Visualizzazione di maggiori dettagli sulle applicazioni installate che sono state rilevate durante un controllo di rete. Quando un'applicazione è selezionata dall'**Elenco** applicazioni, la sezione **Dettagli** fornisce ulteriori informazioni sull'applicazione selezionata.



Screenshot 59: Visualizzazione Software nel Dashboard

Nota

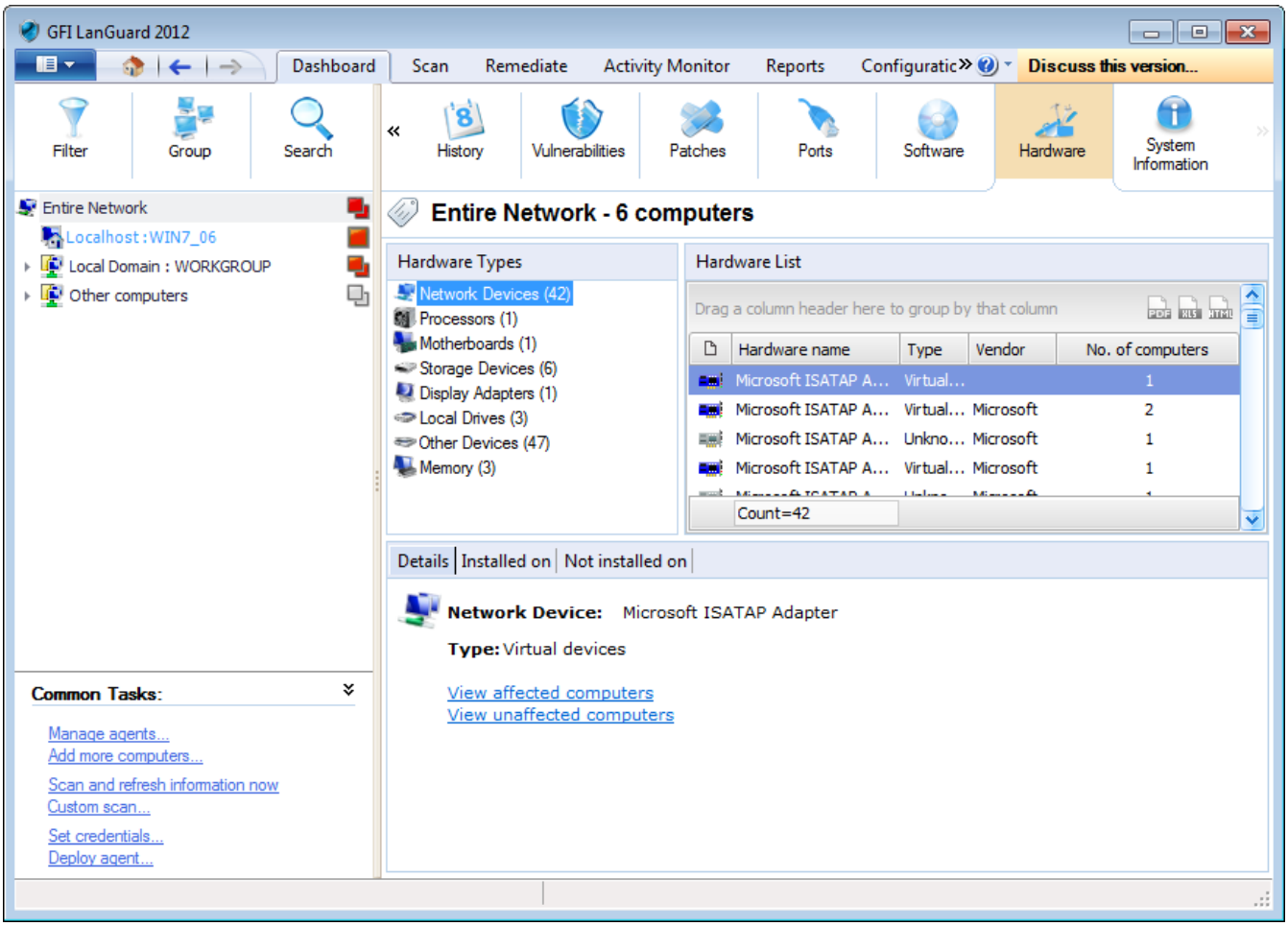
Per raggruppare i dati in base a criteri, trascinare l'intestazione di una colonna nell'area designata.

Nota

Le scansioni senza agente devono temporaneamente eseguire un servizio sul computer remoto. Selezionare **Abilita il controllo completo applicazioni di sicurezza …** per abilitare questo servizio in tutti i profili di scansione senza agente.

6.7.8 Visualizzazione Hardware

Visualizzazione di maggiori informazioni sull'hardware rilevato durante un controllo di rete. Per visualizzare altri dettagli, selezionare hardware dall'elenco.



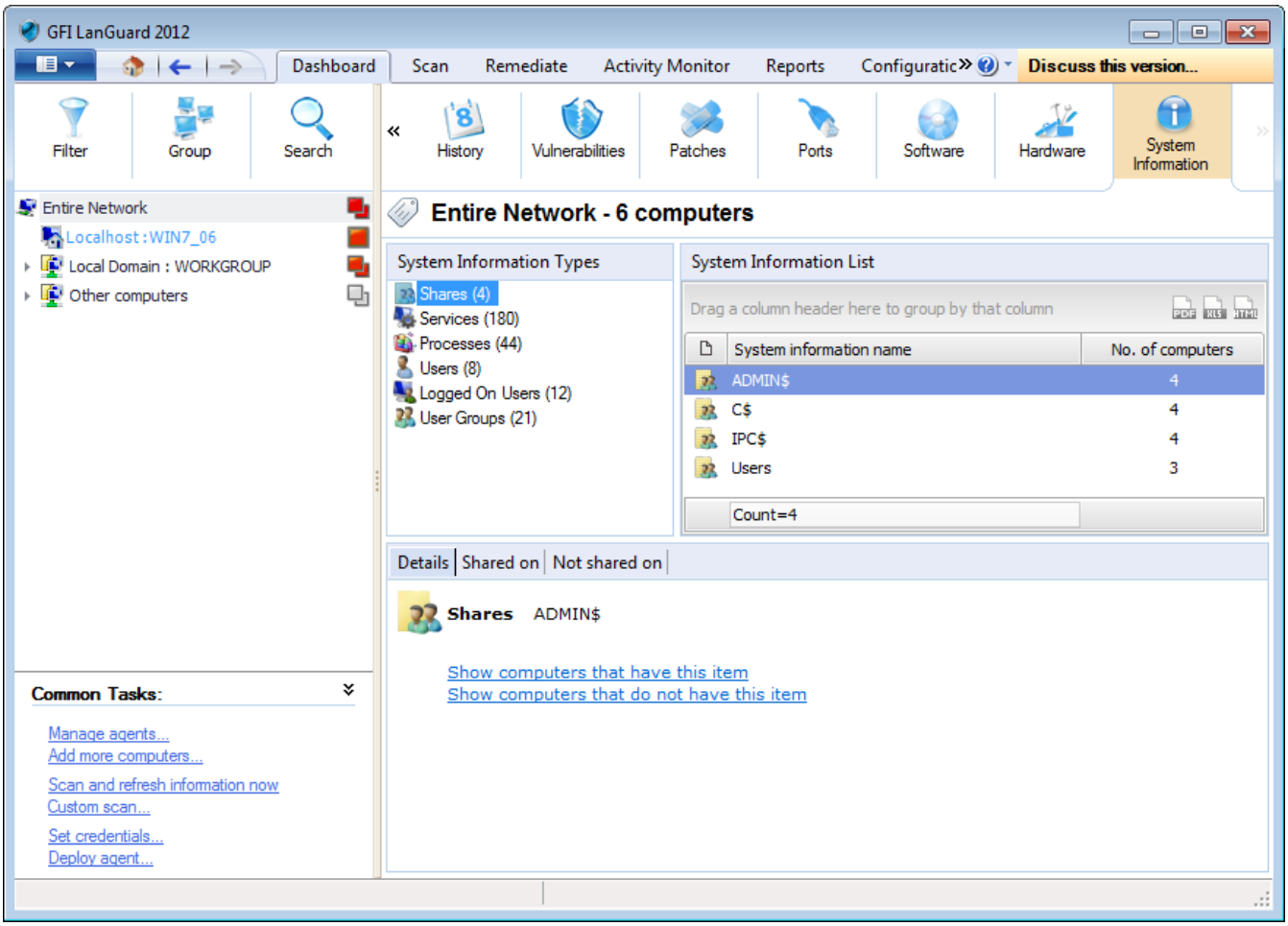
Screenshot 60: Visualizzazione Hardware nel Dashboard

Nota

Per raggruppare i dati in base a criteri, trascinare l'intestazione di una colonna nell'area designata.

6.7.9 Visualizzazione Informazioni di sistema

La scheda **Informazioni di sistema** visualizza informazioni associate al sistema operativo delle destinazioni di scansione.



Screenshot 61: Visualizzazione Informazioni di sistema nel Dashboard

Nota

Per raggruppare i dati in base a criteri, trascinare l'intestazione di una colonna nell'area designata.

7 Interpretazione risultati

Al termine di una scansione di sicurezza della rete, è importante identificare le aree che richiedono immediata attenzione. Utilizzare le informazioni fornite in questo capitolo per stabilire l'approccio corretto di interpretazione e analisi così da ottenere il massimo dai risultati di scansione e applicare le correzioni opportune.

Argomenti del presente capitolo:

7.1 Interpretazione risultati scansione manuale 107
7.2 Caricamento dei risultati dal database 117
7.3 Salvataggio e caricamento dei risultati XML 118

7.1 Interpretazione risultati scansione manuale

Le sezioni **Panoramica risultati scansione** e **Dettagli risultati scansione** nella scheda **Scansione** sono concepite per facilitare al massimo il processo di analisi dei risultati. Utilizzare le informazioni contenute nelle sezioni seguenti per conoscere la modalità di interpretazione dei risultati di scansione e individuare le aree che richiedono attenzione immediata:

- Visualizzazione risultati di scansione
- Valutazione del livello di vulnerabilità
- Valutazione delle vulnerabilità
- Controllo rete e software

7.1.1 Visualizzazione risultati di scansione

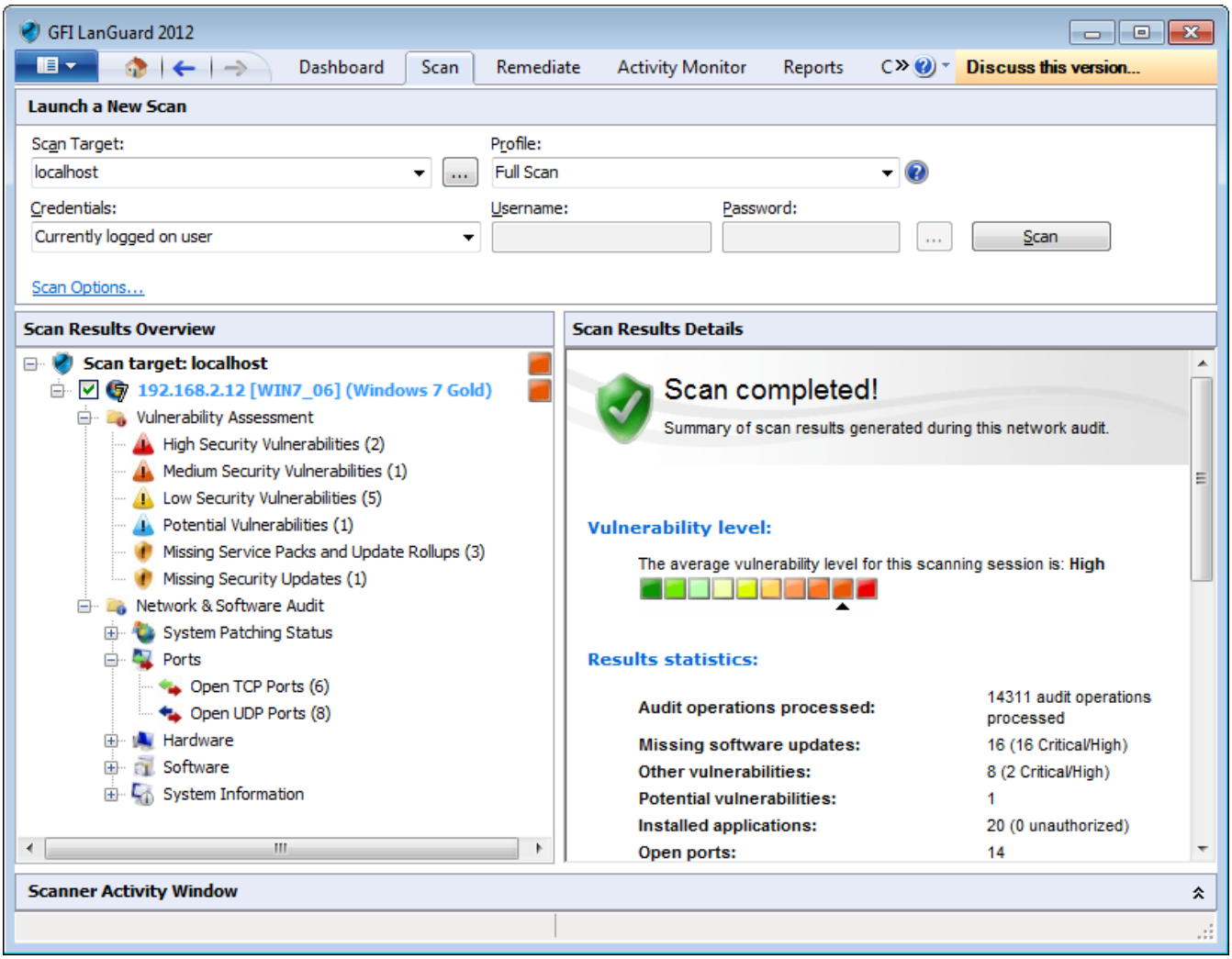
Utilizzare la presente sezione per interpretare i risultati generati dalle scansioni manuali e i risultati archiviati nel database back-end. For more information, refer to Scansioni manuali (page 67).

Per visualizzare i risultati della scansione manuale:

1. Avviare GFI LanGuard e fare clic sulla scheda **Scansione**.

2. Avviare una nuova scansione o caricare i risultati dal database/file. For more information, refer to Caricamento dei risultati dal database (page 117).

3. Al termine, i risultati vengono visualizzati nelle sezioni **Panoramica risultati scansione** e **Dettagli risultati scansione**.



Screenshot 62: Panoramica risultati

Da **Panoramica risultati di scansione**, espandere un nodo del computer per accedere ai risultati ottenuti durante la scansione. I risultati della scansione di sicurezza sono organizzati in due sottonodi contrassegnati come:

- Valutazione delle vulnerabilità
- Controllo rete e software

Mentre la scansione è in corso, ciascun nodo del computer dispone di un'icona che ne categorizza il tempo di risposta. La sottostante tabella illustra i tipi di icone diverse utilizzate da GFI LanGuard per categorizzare il tempo di risposta. La prima icona indica che la scansione è stata inserita nella coda, mentre la seconda icona indica che la scansione è in corso.

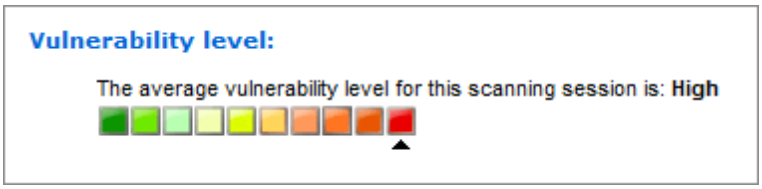
Table 42: Icone tempo di risposta

Categoria	Informazioni	Descrizione
	Risposta rapida	Meno di 25 ms
	Risposta media	Tra 25 e 100 ms
	Risposta lenta	Più di 100 ms

7.1.2 Valutazione del livello di vulnerabilità

Il livello di vulnerabilità GFI LanGuard è una valutazione assegnata a ciascun computer sottoposto a scansione. La valutazione può essere visualizzata da:

- **Dettagli risultati scansione**: questa sezione nella scheda Scansione fornisce la misurazione del livello di vulnerabilità assegnato ai computer/gruppi sottoposti a scansione
- **Dashboard**: la sezione Dashboard fornisce le informazioni relative a computer specifici o gruppi di computer selezionati dalla struttura di computer. Selezionare il computer/gruppo e visualizzare la misurazione delle vulnerabilità dal riquadro di destra. Selezionare Tutta la rete per visualizzare il livello di vulnerabilità per tutte le destinazioni di scansione.



Screenshot 63: Misurazione del livello di vulnerabilità

Metodo di calcolo del livello di vulnerabilità.

Il livello di vulnerabilità viene calcolato utilizzando un sistema di ponderazione. Dopo una scansione, GFI LanGuard raggruppa le vulnerabilità rilevate nelle categorie ordinate in base alla valutazione della gravità:

- Alto
- Medio
- Basso

A ciascuna valutazione viene assegnato un punteggio ponderato, basato sul numero totale di vulnerabilità per categoria.

> **Nota**
>
> Quando non è possibile valutare il livello di vulnerabilità e/o la scansione delle vulnerabilità non è stata eseguita, GFI LanGuard assegna una valutazione di **N/D**.

Punteggi di ponderazione

Table 43: Punteggi di ponderazione del livello di vulnerabilità

Categoria	Numero delle vulnerabilità rilevate	Punteggi
Vulnerabilità di livello alto	1-2 3-5 > 5	8 9 10
Vulnerabilità di livello medio	1-2 3-5 > 5	5 6 7
Vulnerabilità di livello basso	1-2 3-5 > 5	2 3 4

Classificazione dei punteggi

Dopo la categorizzazione delle vulnerabilità rilevate e la generazione di un punteggio per ciascuna categoria, viene generato il livello di vulnerabilità complessiva. Il livello di vulnerabilità è la valutazione di gravità con il punteggio più elevato.

Punteggi livello di vulnerabilità:

- Un punteggio >= **8** risulta in una valutazione di vulnerabilità di livello **alto**
- Un punteggio <= **7** e >= **5** risulta in una valutazione di vulnerabilità di livello **medio**
- Un punteggio <= **4** e >= **1** risulta in una valutazione di vulnerabilità di livello **basso**.

Esempio

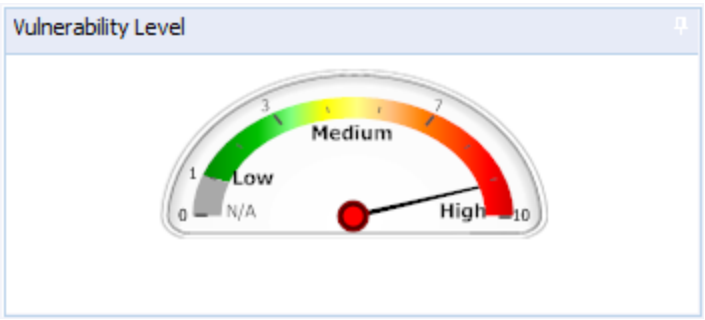
Durante la scansione del computer A, sono state rilevate le vulnerabilità seguenti:

- 3 livelli di vulnerabilità alti
- 8 livelli di vulnerabilità medi
- 5 livelli di vulnerabilità bassi.

Il punteggio per ciascuna categoria è stato calcolato da GFI LanGuard e ha restituito i risultati seguenti:

- 3 livelli di vulnerabilità alti = 9
- 8 livelli di vulnerabilità medi = 7
- 5 livelli di vulnerabilità bassi = 3.

Il livello di vulnerabilità per il computer A è pertanto **ALTO**.

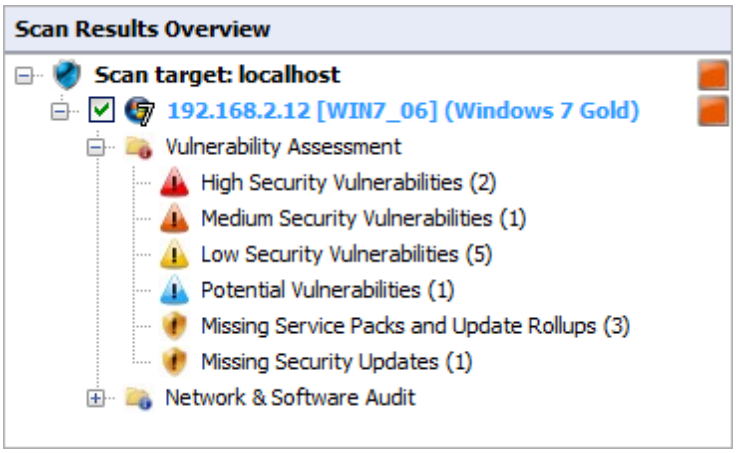


Screenshot 64: Misurazione del livello di vulnerabilità del dashboard

Il livello di vulnerabilità è indicato da una barra grafica colorata:

- Barra rossa = livello di vulnerabilità alto
- Barra verde = livello di vulnerabilità basso.

7.1.3 Valutazione delle vulnerabilità



Screenshot 65: Nodo di valutazione delle vulnerabilità

Fare clic su un nodo di **Valutazione delle vulnerabilità** per visualizzare le vulnerabilità di sicurezza identificate sul computer di destinazione raggruppate per tipo e gravità.

Vulnerabilità di sicurezza di livello alto

Fare clic sui sottonodi **Vulnerabilità di sicurezza di livello alto** o **Vulnerabilità di sicurezza di livello basso** per un elenco delle debolezze rilevate durante il controllo di un dispositivo di destinazione. I gruppi sono descritti nella tabella seguente:

Table 44: Gruppi di vulnerabilità

Gruppo	Descrizione
Posta, FTP, RPC, DNS e varie	Riporta le vulnerabilità scoperte sui server FTP, sui server DNS e sui server di posta SMTP/POP3/IMAP. Sono disponibili collegamenti agli articoli della Microsoft® Knowledge Base o altra documentazione di supporto.
Web	Elenca le vulnerabilità scoperte sui server Web (come i problemi di errata configurazione). I server Web supportati includono Apache, Internet Information Services (IIS®) e Netscape.
Servizi	Elenca le vulnerabilità scoperte nei servizi attivi oltre che l'elenco degli account inutilizzati ancora attivi e accessibili sulle destinazioni sottoposte a scansione.
Registro di sistema	Sono elencate le impostazioni del registro di sistema di un dispositivo di rete sottoposto a scansione. Sono disponibili collegamenti alla documentazione di supporto e brevi descrizioni delle vulnerabilità.
Software	Enumera il software installato sui dispositivi di rete sottoposti a scansione. Sono disponibili collegamenti alla documentazione di supporto e brevi descrizioni delle vulnerabilità.
Rootkit	Enumera le vulnerabilità scoperte in seguito all'installazione di un rootkit sui dispositivi di rete sottoposti a scansione. Sono disponibili collegamenti alla documentazione di supporto e brevi descrizioni delle vulnerabilità.

Potenziali vulnerabilità

Selezionare il sottonodo **Potenziali vulnerabilità** per visualizzare gli elementi dei risultati della scansione classificati come possibili debolezze di rete. Nonostante non siano classificate come vulnerabilità, queste voci dei risultati della scansione richiedono comunque un elevato grado di attenzione dal momento che possono essere sfruttate da utenti con intenzioni maligne.

Ad esempio, durante la vulnerabilità di scansione, GFI LanGuard enumera tutti i modem installati e configurati sui computer di destinazione. Se inutilizzati, i modem non rappresentano una minaccia per la rete. Tuttavia, se sono connessi a una linea telefonica, i modem possono essere utilizzati per ottenere accesso non autorizzato e non monitorato a Internet. Ciò significa che gli utenti possono

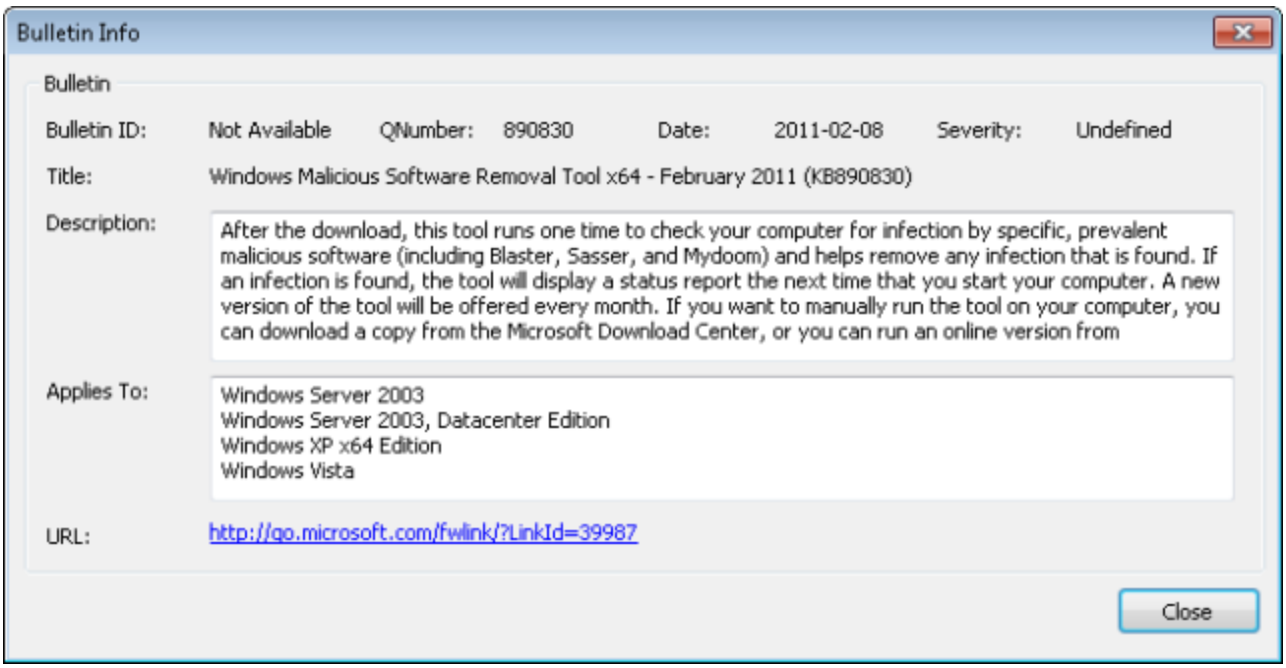
aggirare il perimetro di sicurezza aziendale compresi firewall, antivirus, valutazione dei siti Web e blocco dei contenuti Web. Esponendo l'infrastruttura IT aziendale a una serie di minacce compresi attacchi di hacker. GFI LanGuard Considera i modem installati come possibili minacce e li elenca nel sottonodo **Potenziali vulnerabilità**.

Service pack mancanti

Fare clic su **Service pack e aggiornamenti cumulativi mancanti** o sui sottonodi **Aggiornamenti di sicurezza mancanti** per verificare eventuali patch o aggiornamenti software mancanti. Per un elenco completo dei service pack e delle patch mancanti che possono essere identificati da GFI LanGuard, fare riferimento a http://go.gfi.com/?pageid=ms_app_fullreport

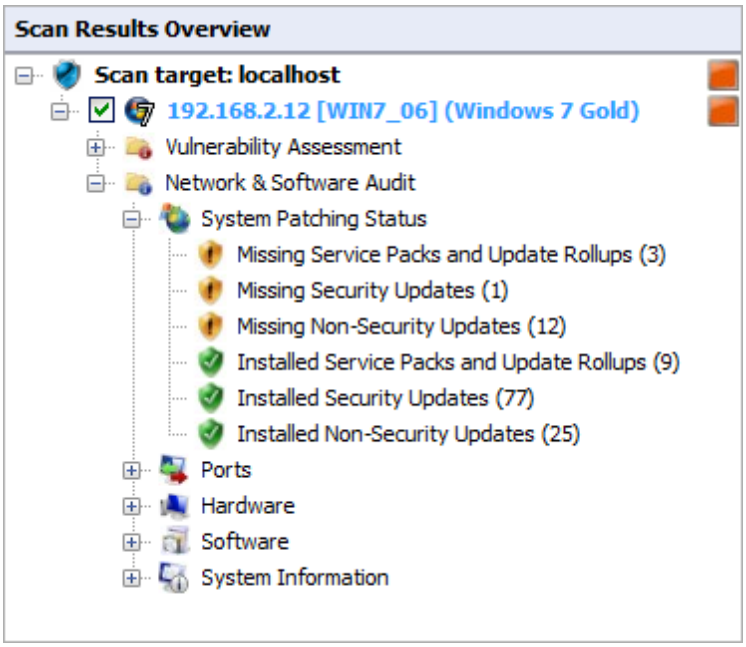
Info bollettino.

Per accedere alle informazioni sul bollettino, fare clic con il tasto destro del mouse sul relativo service pack e selezionare **Ulteriori dettagli>Info bollettino**.


Bulletin Info
Bulletin
Bulletin ID:
Not Available
QNumber:
890830
Date:
2011-02-08
Severity:
Undefined
Title:
Windows Malicious Software Removal Tool x64 - February 2011 (KB890830)
Description:
After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from
Applies To:
Windows Server 2003
Windows Server 2003, Datacenter Edition
Windows XP x64 Edition
Windows Vista
URL:
http://go.microsoft.com/fwlink/?LinkId=39987
Close

Screenshot 66: Finestra di dialogo Info bollettino

7.1.4 Controllo rete e software



Screenshot 67: Nodo Controllo rete e software

Selezionare **Controllo rete e software** per visualizzare le vulnerabilità di sicurezza identificate sulle destinazioni sottoposte a scansione. In questa sezione, le vulnerabilità sono raggruppate per tipo e gravità.

Stato dell'applicazione di patch al sistema

Selezionare **Stato dell'applicazione di patch al sistema** per visualizzare tutte le patch mancanti e installate in un computer di destinazione. I collegamenti disponibili sono:

- Service pack e aggiornamenti cumulativi mancanti
- Aggiornamenti di sicurezza mancanti
- Aggiornamenti non di sicurezza mancanti
- Service pack e aggiornamenti cumulativi installati
- Aggiornamenti di sicurezza installati
- Aggiornamenti non di sicurezza installati.

Scan Results Details
System Patching Status
Select one of the following system patching status categories bellow
Missing Service Packs and Update Rollups (3)
Allows you to analyze the missing service packs information
Missing Security Updates (1)
Allows you to analyze the missing security updates information
Missing Non-Security Updates (12)
Allows you to analyze the non-security updates information
Installed Service Packs and Update Rollups (9)
Allows you to analyze the installed service packs information
Installed Security Updates (77)
Allows you to analyze the installed security update information
Installed Non-Security Updates (25)
Allows you to analyze the installed non-security updateinformation

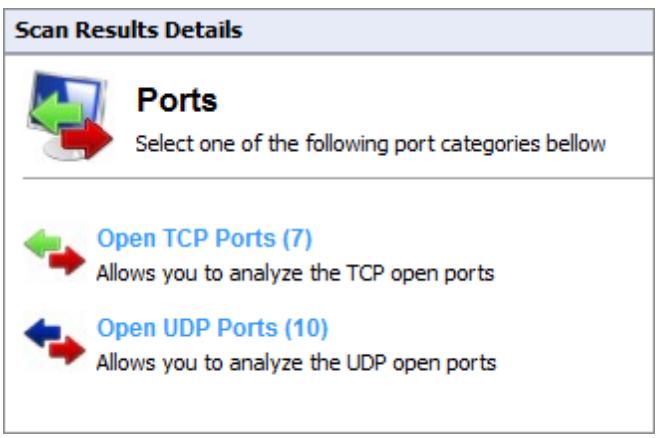
Screenshot 68: Stato patch di sistema

Porte

Selezionare **Porte** per visualizzare tutte le porte TCP e UDP rilevate durante una scansione. Quando viene trovata aperta una porta comunemente sfruttata, GFI LanGuard la contrassegna in rosso.

> **Nota**
>
> Alcuni prodotti software possono utilizzare le medesime porte dei trojan più noti. Per una sicurezza aggiuntiva, GFI LanGuard identificherà queste porte come minacce.

Oltre a rilevare le porte aperte, GFI LanGuard utilizza la tecnologia delle impronte digitali del servizio per analizzare il servizio in esecuzione dietro la porta aperta rilevata. Con le impronte digitali del servizio, GFI LanGuard può rilevare se un software malintenzionato sta utilizzando la porta aperta rilevata.


Scan Results Details
Ports
Select one of the following port categories bellow
Open TCP Ports (7)
Allows you to analyze the TCP open ports
Open UDP Ports (10)
Allows you to analyze the UDP open ports

Screenshot 69: Tutte le porte UDP e TCP rilevate durante una scansione

Hardware

Per visualizzare tutti i dettagli rilevati dal controllo hardware, selezionare **Hardware**. Il controllo hardware, inoltre, visualizza informazioni quali indirizzi MAC, indirizzi IP, tipo di dispositivo, fornitore dispositivo ecc. La sottostante tabella descrive i gruppi di informazioni hardware:

Table 45: Informazioni hardware dal controllo

Informazioni	Descrizione
Dispositivi di rete	Include informazioni relative a tutti i dispositivi fisici, virtuali ed enumerati dal software.
Unità locali	Include informazioni sulle unità locali quali spazio su disco disponibile e tipo di file system.
Processori	Include informazioni relative al processore di un computer di destinazione, come il nome del fornitore e la velocità del processore.
Scheda madre	Include informazioni relative alla scheda madre del computer di destinazione, come nome prodotto, produttore, versione e numero di serie.
Dettagli memoria	Include informazioni relative all'allocazione della memoria di un computer di destinazione, come la memoria virtuale/fisica disponibile.
Dettagli archiviazione	Include informazioni relative all'archiviazione di un computer di destinazione, come unità floppy, CD/ROM e dischi rigidi.
Schede video	Include informazioni relative alla visualizzazione e alle periferiche video di un computer di destinazione, come il produttore del dispositivo.
Altri dispositivi	Include informazioni sui dispositivi che non rientrano nelle categorie di cui sopra, come tastiera, porte, mouse e altre periferiche human interface.

Software

Per visualizzare tutti i dettagli coinvolti nel controllo software, selezionare **Software**. Il controllo software, inoltre, visualizza informazioni quali:

- Nome applicazione
- Autore
- Versione.

La sottostante tabella descrive i gruppi di informazioni hardware:

Table 46: Informazioni software dal controllo

Icona	Descrizione
Applicazioni generali	Enumera il software installato sulle destinazioni di scansione.
Applicazioni antivirus	Elenca i motori antivirus installati sulle destinazioni di scansione.
Applicazioni di messaggistica istantanea	Elenca tutte le istanze di applicazioni di messaggistica istantanea rilevate sulle destinazioni di scansione.
Applicazioni di gestione patch	Elenca tutte le applicazioni di gestione delle patch installate, rilevate sulle destinazioni di scansione nel corso di una scansione.
Applicazioni browser Web	Contiene le destinazioni scansionate dove sono installati browser Internet.
Applicazioni firewall	Enumera informazioni sulle applicazioni firewall installate nelle destinazioni di scansione.
Applicazioni antiphishing	Elenca le informazioni relative ai motori anti-phishing installati nelle destinazioni di scansione.
Applicazioni client VPN	Informazioni dei client Virtual Private Network installati nelle destinazioni di scansione.
Applicazioni Peer-To-Peer	Visualizza le applicazioni Peer-To-Peer installate nelle destinazioni di scansione.

Informazioni di sistema

Per visualizzare tutti i dettagli relativi al sistema operativo installato in un computer di destinazione, selezionare **Informazioni di sistema**. La sottostante tabella descrive i gruppi di informazioni di sistema:

Table 47: Informazioni di sistema da un controllo

Categoria	Informazioni	Identifica
Condivisioni	» Nome condivisione » Nota condivisione (dettagli aggiuntivi sulla condivisione). » Cartella condivisa sul computer di destinazione » Autorizzazione e diritti di accesso di condivisione » Autorizzazione e diritti di accesso NTFS.	» Utenti che condividono dischi rigidi, condivisioni con autorizzazioni di accesso deboli o configurate in modo errato. » Cartelle di avvio e file di sistema simili accessibili dagli utenti non autorizzati o per mezzo di account di utenti privi di privilegi di amministratore ma autorizzati a eseguire il codice sui computer di destinazione. » Condivisioni non necessarie o inutilizzate.
Criterio password	» Lunghezza minima password » Lunghezza massima password » Data di scadenza minima della password » Imponi disconnessione » Cronologia password	» Comando di chiusura configurato in modo errato » Criteri di imposizione del livello di sicurezza della password
Criterio controllo di protezione	» Controllo eventi accesso account » Controllo gestione account » Controllo accesso al servizio directory » Controllo eventi di accesso » E molto altro...	» Buchi o falle di sicurezza **Nota** Per visualizzare il criterio controllo di protezione, abilitare il controllo sui computer di destinazione. For more information, refer to Scansioni manuali (page 67).
Registro di sistema	» Proprietario registrato » Organizzazione registrata » Nome prodotto » Numero build attuale	» Impostazioni hardware e software come i driver e le applicazioni da lanciare automaticamente all'avvio del sistema
Nomi NETBIOS	» Servizio workstation » Nome dominio » Controller di dominio » Servizio file server	» Computer anomali » Configurazioni errate

Categoria	Informazioni	Identifica
Gruppi	» Operatori account » Amministratori » Operazioni di backup » Ospite	» Configurazioni errate » Errori di sicurezza dovuti a gruppi di utenti obsoleti o anomali
Utenti	» Nome completo » Privilegio » Contrassegni » Accesso	» Account utenti predefiniti, obsoleti o anomali
Utenti connessi	» Elenco di utenti connessi	» Utenti autorizzati e non autorizzati attualmente connessi ai computer
Sessioni	» Elenco di host connessi in modalità remota al computer di destinazione durante la scansione	» Connessioni remote autorizzate e non autorizzate
Servizi	» Elenco di servizi attivi	» Processi maligni o anomali; servizi ridondanti
Processi	» Elenco di processi attivi	» Processi maligni o anomali
TOD (ora del giorno) in remoto)	» Ora della workstation remota, del server o del computer portatile	» Incoerenze orarie e impostazioni regionali » Configurazioni errate

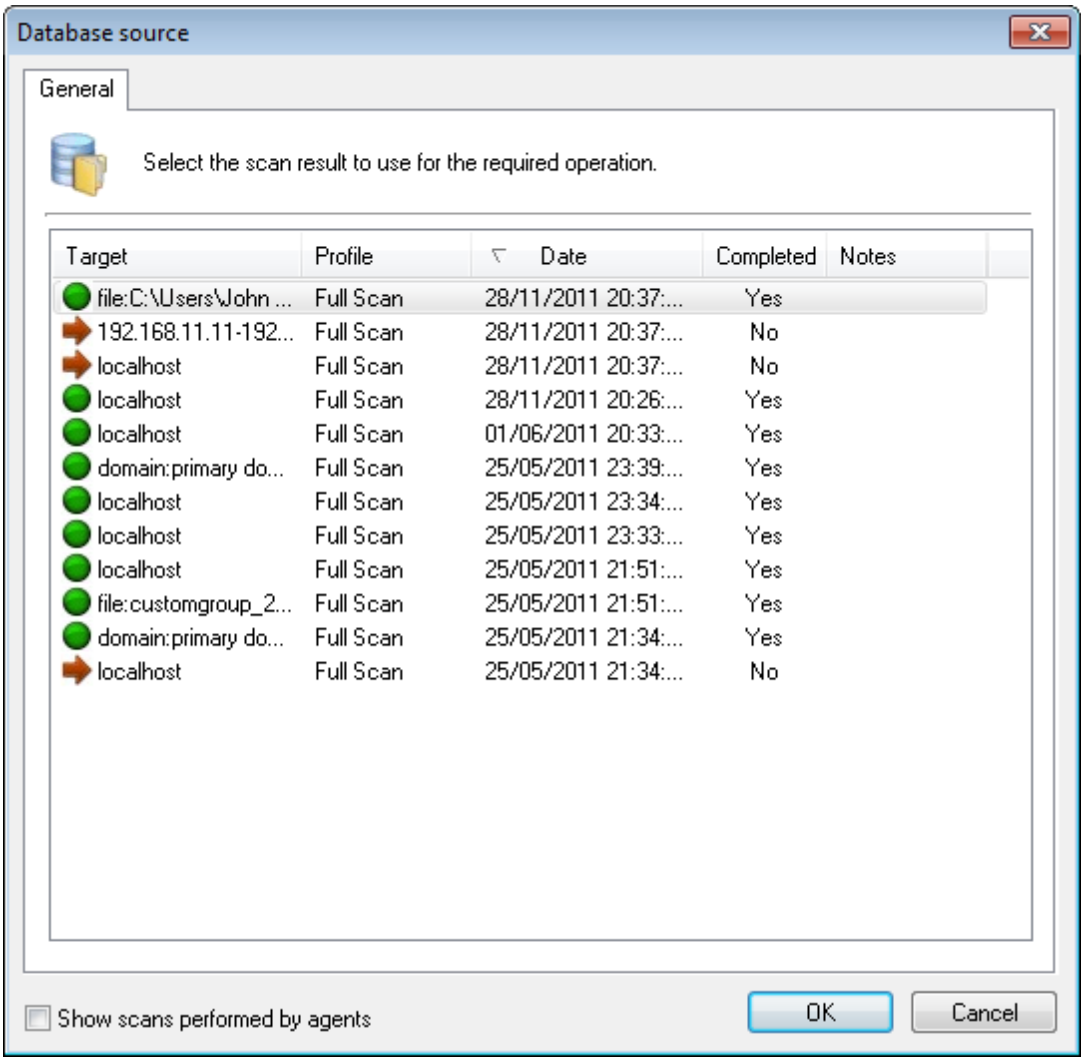
7.2 Caricamento dei risultati dal database

Per impostazione predefinita, i risultati della scansione salvati vengono conservati all'interno di un database. GFI LanGuard salva i dati dei risultati delle ultime 10 scansioni eseguite per ciascun profilo di scansione. È possibile configurare il numero di risultati della scansione salvati in un file di database. For more information, refer to Configurazione opzioni di manutenzione database (page 184).

Per caricare i risultati della scansione salvati dal database back-end o da file XML:

1. Avviare GFI LanGuard.

2. Fare clic sul pulsante GFI LanGuard> **File > Carica risultati di scansione da > Database…**



Screenshot 70: Risultati della scansione ricaricati

3. Selezionare il risultato di scansione salvato e fare clic su **OK**.

4. Analisi risultati caricati. Per ulteriori informazioni sull'interpretazione dei risultati, fare riferimento alle seguenti sezioni:

- valutazione delle vulnerabilità
- Controllo rete e software.

7.3 Salvataggio e caricamento dei risultati XML

I risultati della scansione sono una fonte di informazioni dal valore inestimabile per gli amministratori di sistema. I risultati di GFI LanGuard vengono archiviati in un database SQL Server® o Access™. In aggiunta, i risultati della scansione possono anche essere esportati in formato XML.

Per salvare i risultati di scansione in un file XML:

1. Avviare GFI LanGuard.

2. Eseguire una scansione manuale. For more information, refer to Scansioni manuali (page 67).

3. Una volta completata la scansione, fare clic sul pulsante GFI LanGuard**> File > Salva risultati di scansione**.

4. Individuare la posizione dove salvare l'XML e fare clic su **Salva**.

Per caricare i risultati della scansione salvati da un file XML:

1. Fare clic sul pulsante GFI LanGuard**> File > Carica risultati di scansione da> File XML…**
2. Localizzare i risultati della scansione da caricare e fare clic su **OK**.
3. Analizzare i risultati caricati.

> **Nota**
>
> Per ulteriori informazioni sull'interpretazione dei risultati, fare riferimento alle sezioni seguenti:
>
> - Valutazione delle vulnerabilità
> - Controllo rete e software

8 Riparazione vulnerabilità

GFI LanGuard consente di riparare manualmente o automaticamente le vulnerabilità nei computer della rete. Utilizzare le informazioni contenute in questo capitolo per sapere come configurare e gestire le operazioni di riparazione al fine di mantenere un livello di sicurezza elevato tra le destinazioni di scansione.

Argomenti del presente capitolo:

8.1 Riparazione automatica 120

8.2 Riparazione manuale 143

8.1 Riparazione automatica

La riparazione automatica consente di scaricare e distribuire automaticamente le patch mancanti, oltre che disinstallare automaticamente le applicazioni non autorizzate durante le operazioni pianificate.

IMPORTANTE

La riparazione automatica e la disinstallazione delle applicazioni non autorizzate funzionano solo sui profili di scansione che rilevano le patch mancanti e/o le applicazioni installate.

Attività di riparazione automatica:

- Rivedere le Considerazioni di riparazione automatica
- Configurazione distribuzione automatica aggiornamenti mancanti
- Configurazione disinstallazione automatica applicazioni non autorizzate
- Configurazione delle opzioni di riparazione automatica
- Configurazione Wake-on-LAN sui computer client
- Configurazione opzioni di riavvio e arresto utente finale
- Definizione dei messaggi di riparazione automatica
- Configurazione riparazione automatica agenti

8.1.1 Note sulla riparazione automatica

Prima di abilitare e configurare le opzioni di riparazione automatica, rivedere le seguenti note relative a:

- Installazione del software
- Disinstallazione del software

Installazione del software

Testare sempre le patch in un ambiente di prova prima della distribuzione.

Per impostazione predefinita, gli aggiornamenti Microsoft® non sono configurati per la distribuzione automatica. Approvare manualmente ciascuna patch (dopo averla testata) o impostare tutti gli aggiornamenti Microsoft® come approvati.

Disinstallazione del software

Per disinstallare il software, è necessario seguire un procedimento in tre fasi per identificare se l'applicazione selezionata supporta la disinstallazione invisibile:

Table 48: Fasi di riparazione automatica

Fase	Descrizione
Fase°1	Selezionare l'applicazione da disinstallare in automatico.
Fase°2	Assicurarsi che l'applicazione supporti la disinstallazione invisibile. Tale verifica può essere effettuata tentando la disinstallazione in remoto dell'applicazione. Questa operazione viene chiamata processo di convalida.
Fase°3	Configurare una scansione pianificata che rimuoverà l'applicazione non autorizzata. Questa operazione può essere eseguita in automatico (tramite gli agenti) o manualmente (procedura senza agente).

La riparazione automatica e la disinstallazione delle applicazioni non autorizzate funzionano solo sui profili di scansione che rilevano le patch mancanti e/o le applicazioni installate.

8.1.2 Configurazione della distribuzione automatica degli aggiornamenti mancanti

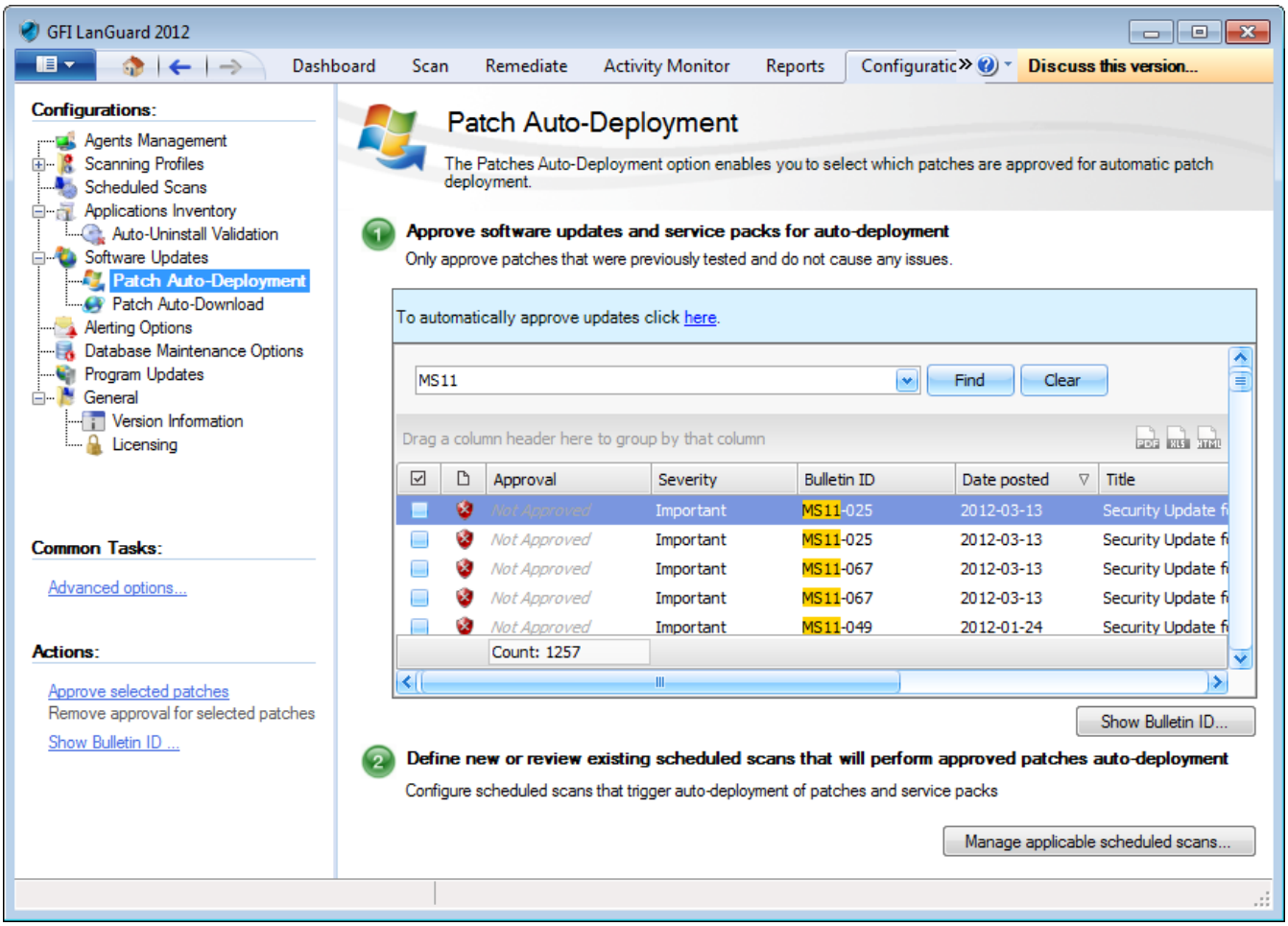
GFI LanGuard viene fornito completo di una funzione di distribuzione automatica delle patch che consente di distribuire automaticamente le patch e i service pack mancanti in tutte le 38 lingue supportate dai prodotti Microsoft®. GFI LanGuard supporta anche l'esecuzione di patch di terze parti (non Microsoft®). Per un elenco completo delle applicazioni di terze parti supportate, visitare: http://go.gfi.com/?pageid=3p_fullreport. Fare riferimento alla seguente sezione per informazioni relative a:

- Abilitazione distribuzione automatica patch
- Configurazione delle opzioni avanzate di Distribuzione automatica patch
- Configurazione delle impostazioni di download automatico delle patch

Abilitazione distribuzione automatica patch

Per configurare la distribuzione automatica delle patch:

1. Fare clic sulla scheda **ConfigurazioneAggiornamenti software > Distribuzione automatica patch**.
2. Nel riquadro di destra, selezionare le patch da distribuire automaticamente.



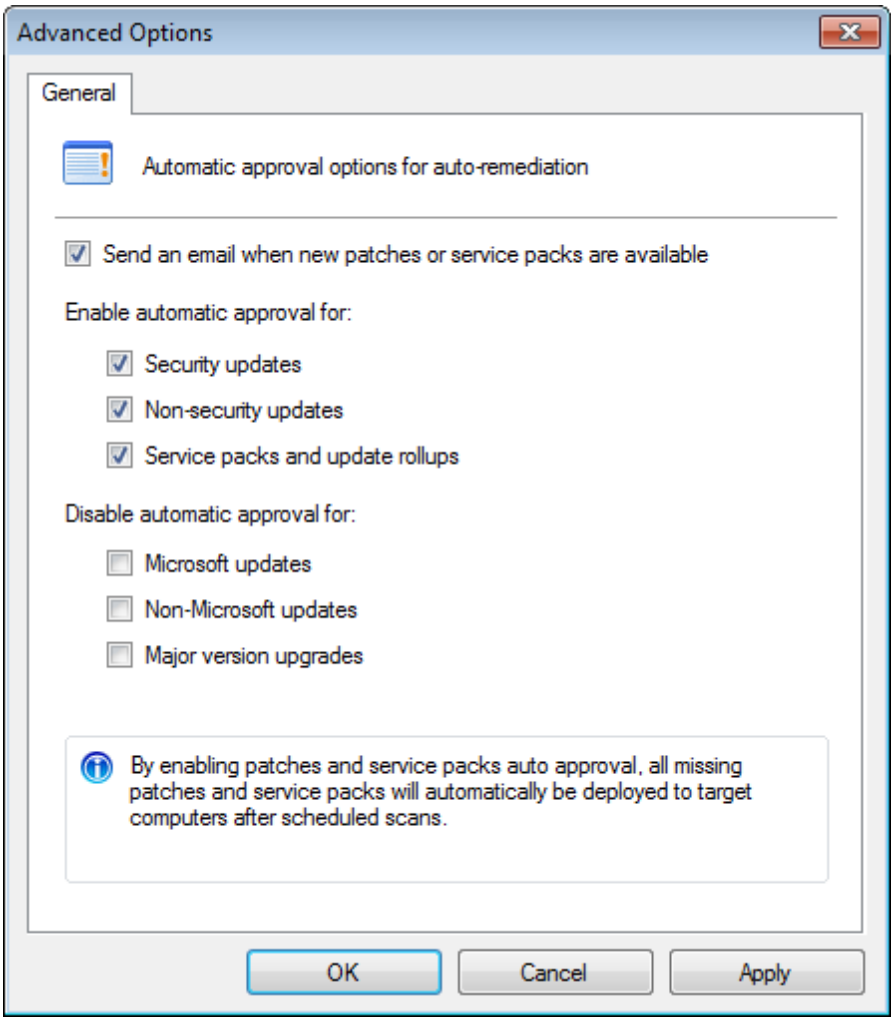
Screenshot 71: Distribuzione automatica delle patch

> **Nota**
>
> Immettere un criterio di ricerca quindi fare clic su **Trova** per cercare l'applicazione specifica.

Configurazione delle opzioni avanzate di Distribuzione automatica patch

Per configurare la riparazione automatica:

1. Selezionare la scheda **ConfigurazioneAggiornamenti software > Distribuzione automatica patch** e in **Attività comuni**, selezionare **Opzioni avanzate**.


Advanced Options
General
Automatic approval options for auto-remediation
Send an email when new patches or service packs are available
Enable automatic approval for:
Security updates
Non-security updates
Service packs and update rollups
Disable automatic approval for:
Microsoft updates
Non-Microsoft updates
Major version upgrades
By enabling patches and service packs auto approval, all missing patches and service packs will automatically be deployed to target computers after scheduled scans.
OK
Cancel
Apply

Screenshot 72: Opzioni avanzate di distribuzione automatica delle patch

2. Configurare le opzioni seguenti:

Table 49: Opzioni avanzate di distribuzione automatica delle patch

Opzione	Descrizione
Inviare un messaggio e-mail quando nuove patch o nuovi service pack sono disponibili.	Inviare un messaggio e-mail quando vengono identificate nuove patch.
Abilita approvazione automatica per:	Gli aggiornamenti selezionati vengono scaricati automaticamente e installati nei computer di destinazione. Selezionare dalle opzioni seguenti: » Aggiornamenti di sicurezza » Aggiornamenti non di sicurezza » Service pack e aggiornamenti cumulativi.

Opzione	Descrizione
Disabilita approvazione automatica per	Gli aggiornamenti selezionati vengono scaricati ma non installati automaticamente nei computer di destinazione. Selezionare dalle opzioni seguenti: » Aggiornamenti Microsoft® » Aggiornamenti non Microsoft® » Aggiornamenti versione principale. **Nota** Gli aggiornamenti possono essere installati manualmente da **Centro riparazioni**. For more information, refer to Utilizzo del Centro riparazioni (page 143).

3. Selezionare le caselle di controllo relative e fare clic su **OK** per salvare le modifiche.

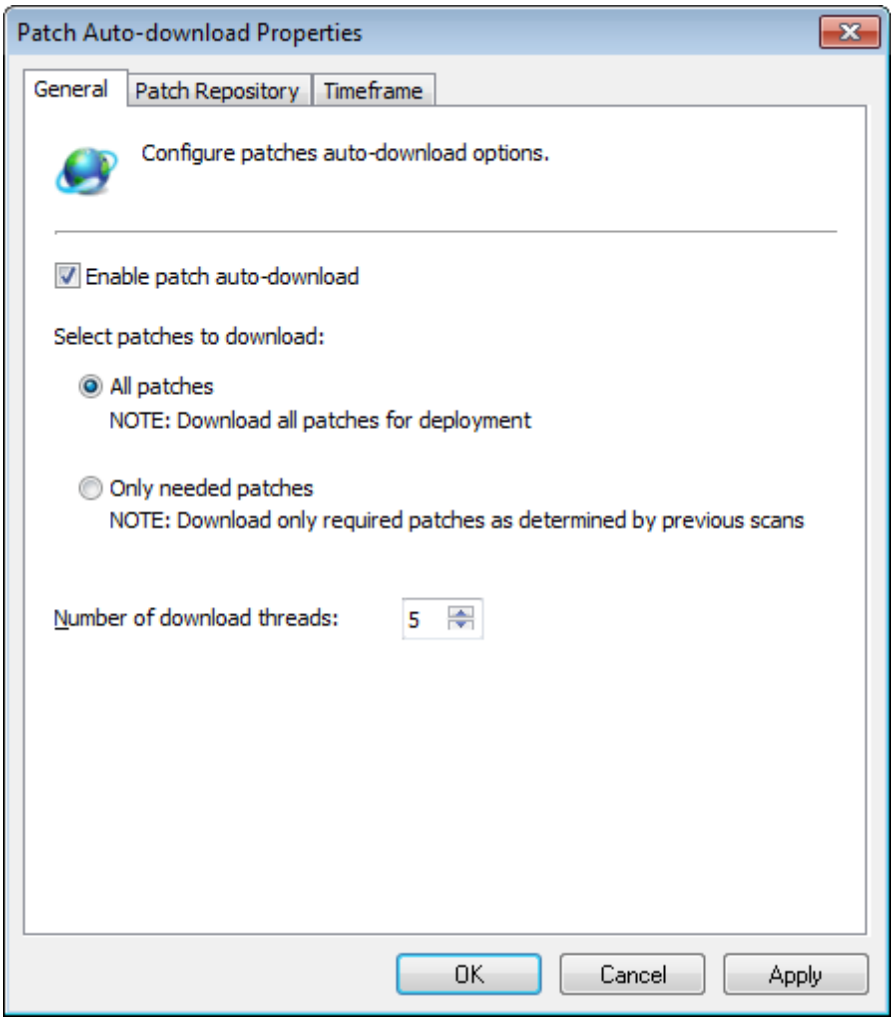
Configurazione delle impostazioni di download automatico delle patch

GFI LanGuard viene fornito con la funzione di download automatico delle patch che consente di scaricare automaticamente le patch e i service pack mancanti in tutte le 38 lingue supportate dai prodotti Microsoft®. In aggiunta, è anche possibile pianificare il download automatico delle patch specificando l'intervallo di tempo per il download delle patch.

Per configurare il download automatico delle patch:

1. Fare clic sulla scheda **ConfigurazioneAggiornamenti software > Download automatico patch**.

2. Dal riquadro a destra, selezionare il collegamento.

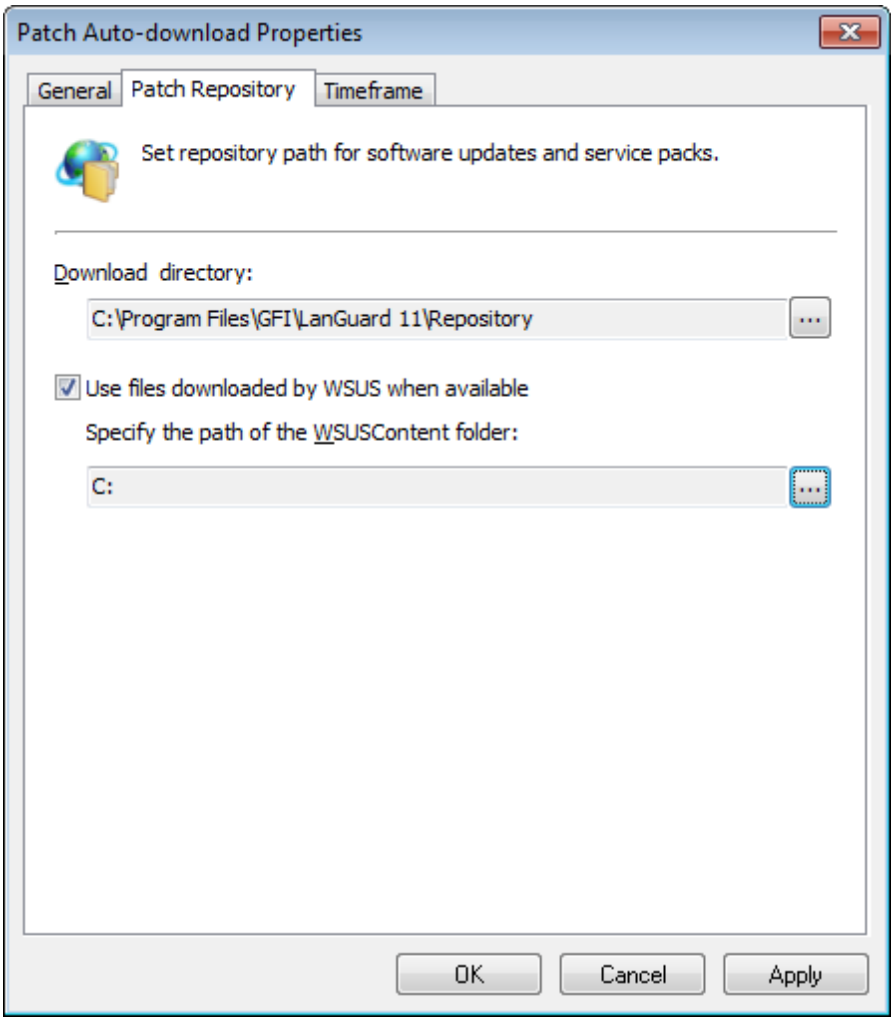


Screenshot 73: Configurazione proprietà di download automatico patch

3. Nella scheda **Generale**, selezionare **Tutte le patch** o **Solo le patch necessarie**.

Nota

Selezionando **Tutte le patch**, vengono scaricate tutte le patch rilasciate da Microsoft®, senza tener conto del fatto che la loro distribuzione sia necessaria o meno. L'opzione Solo le patch necessarie scarica solo le patch da distribuire necessariamente.



Screenshot 74: Impostazioni di archivio patch

4. Per cambiare la posizione di salvataggio delle patch scaricate, fare clic sulla scheda **Archivio patch** e specificare i dettagli richiesti.

5. Selezionare **Usa file scaricati da WSUS se disponibili**, se si utilizza una configurazione esistente di WSUS.

6. Per modificare l'intervallo di tempo durante il quale vengono eseguiti i download delle patch, fare clic sulla scheda **Intervallo di tempo** e specificare i dettagli necessari.

7. Fare clic su **Applica** e su **OK**.

8.1.3 Configurazione della disinstallazione automatica delle applicazioni non autorizzate

La disinstallazione automatica delle applicazioni richiede che le applicazioni contrassegnate come non autorizzate per gli specifici profili di scansione vengano prima convalidate per una corretta disinstallazione su un computer di prova. In seguito, i profili di scansione contenenti applicazioni contrassegnate come non autorizzate vengono configurati per eseguire la disinstallazione automatica delle applicazioni non autorizzate rilevate.

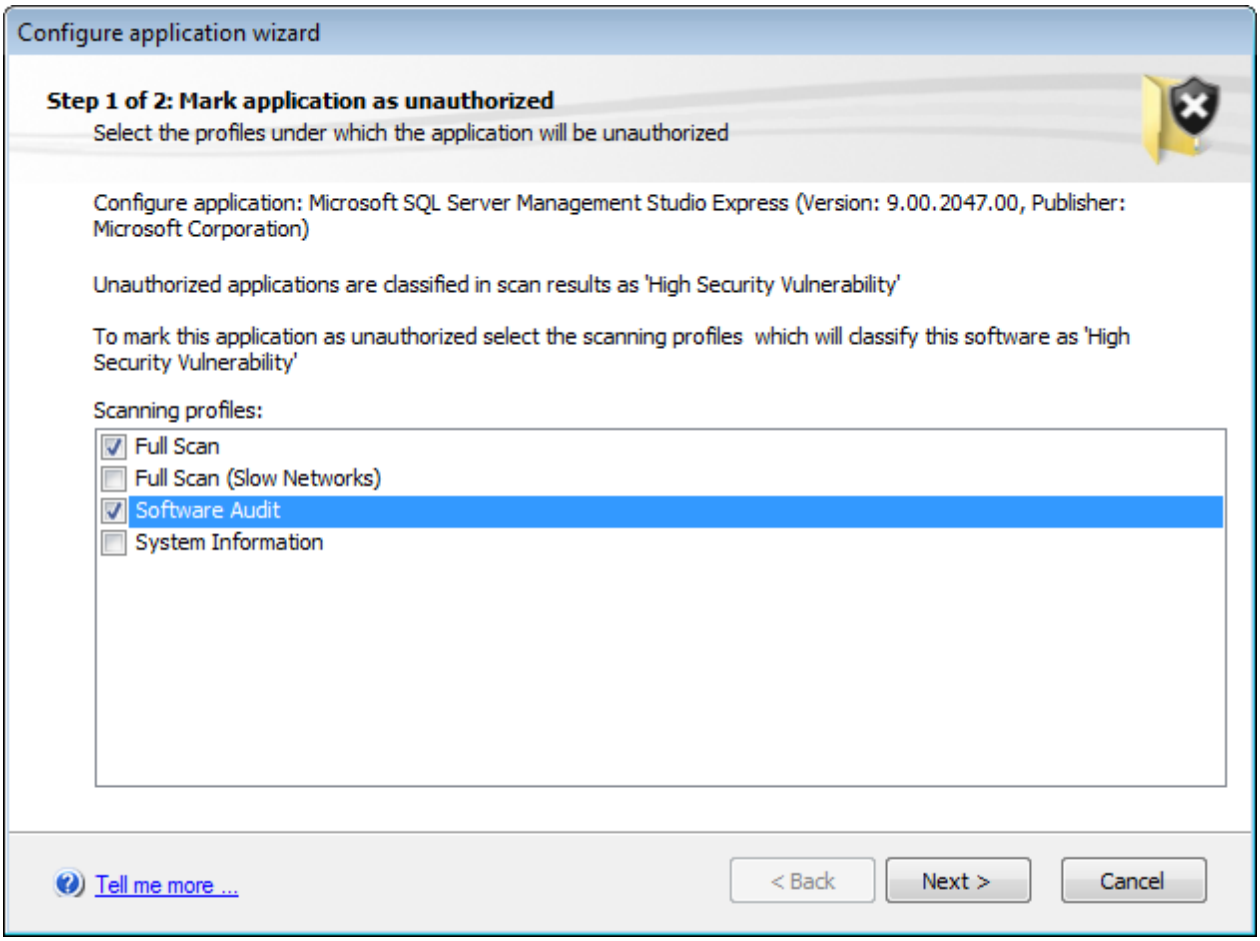
L'inventario delle applicazioni di GFI LanGuard fornisce un elenco di tutte le applicazioni rilevate durante le scansioni precedenti. L'elenco viene utilizzato per specificare le applicazioni non autorizzate. È anche possibile aggiungere manualmente le applicazioni all'elenco. A tal fine, specificare il nome completo e un nome parziale, un nome generico specifico o parte del nome di un'applicazione. GFI LanGuard esegue automaticamente la scansione dell'elenco di applicazioni e rileva i nomi parziali. Per ulteriori informazioni, fare riferimento alle seguenti sezioni:

- Impostazione di un'applicazione come non autorizzata
- Aggiunta di nuove applicazioni all’elenco di quelle non autorizzate
- Convalida applicazioni non autorizzate per disinstallazione automatica
- Gestione delle scansioni pianificate applicabili

Impostazione di un'applicazione come non autorizzata

1. Fare clic sulla scheda **Configurazione**, selezionare il sottonodo > **Inventario applicazioni**.

2. Dall’elenco di applicazioni rilevate sulla destra, fare doppio clic sull’applicazione da impostare come non autorizzata.


Configure application wizard
Step 1 of 2: Mark application as unauthorized
Select the profiles under which the application will be unauthorized
Configure application: Microsoft SQL Server Management Studio Express (Version: 9.00.2047.00, Publisher: Microsoft Corporation)
Unauthorized applications are classified in scan results as 'High Security Vulnerability'
To mark this application as unauthorized select the scanning profiles which will classify this software as 'High Security Vulnerability'
Scanning profiles:
Full Scan
Full Scan (Slow Networks)
Software Audit
System Information
Tell me more ...
< Back
Next >
Cancel

Screenshot 75: Applicazione non autorizzata

3. Selezionare il profilo di scansione in relazione al quale questa applicazione verrà impostata come non autorizzata e fare clic su **Avanti**.

4. GFI LanGuard è in grado di associare i nomi parziali con le voci già presenti in elenco. Di conseguenza, il sistema richiederà se si desidera confermare l'applicazione delle stesse modifiche anche alle applicazioni aventi un nome parzialmente simile.

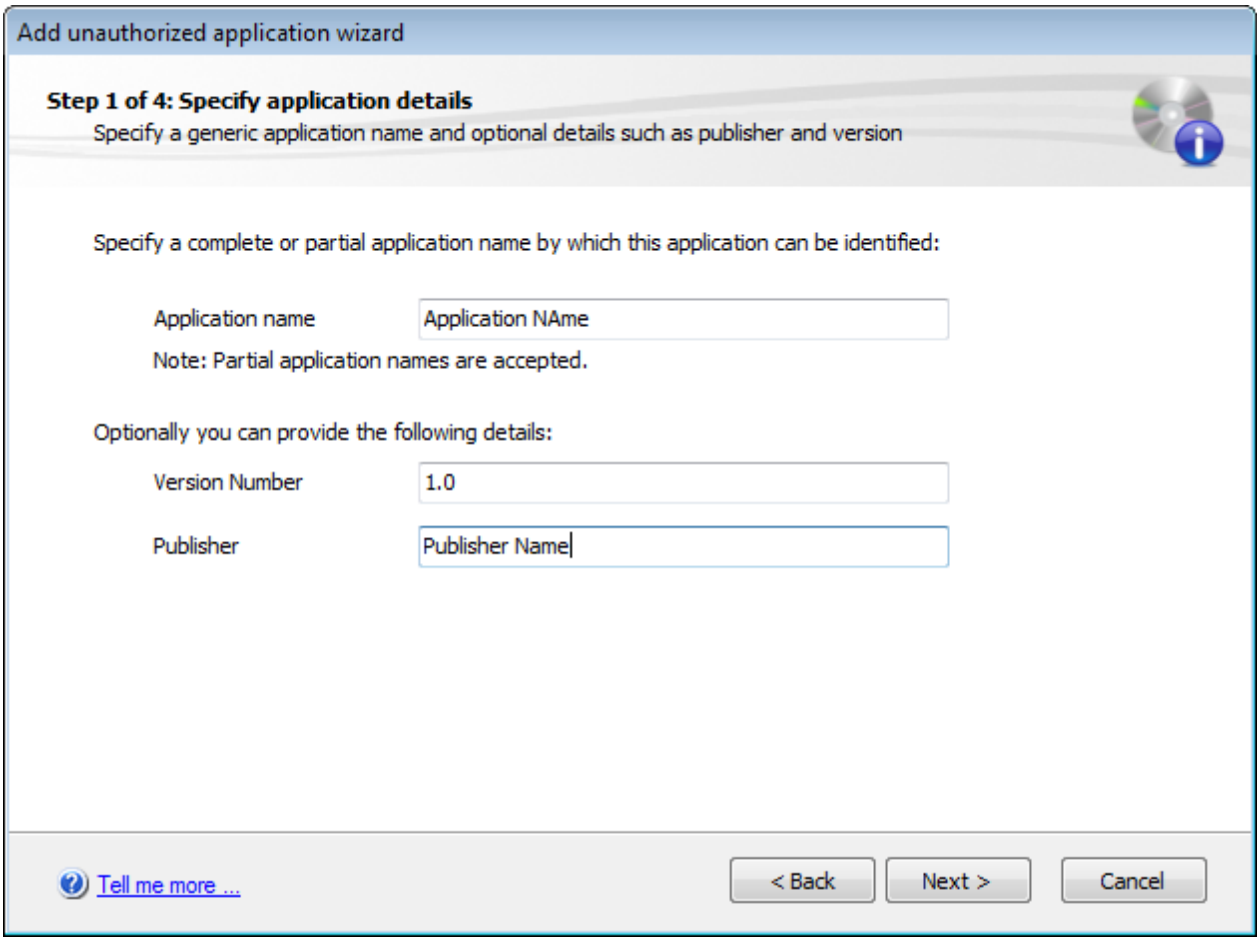
5. Fare clic su **Fine** per completare le impostazioni.

Aggiunta di nuove applicazioni all’elenco di quelle non autorizzate

1. Fare clic sulla scheda **Configurazione**, selezionare il sottonodo > **Inventario applicazioni**.

2. In **Attività comuni**, fare clic su **Aggiungi una nuova applicazione**.

3. Nella schermata di benvenuto, fare clic su **Avanti** per procedere.


Add unauthorized application wizard
Step 1 of 4: Specify application details
Specify a generic application name and optional details such as publisher and version
Specify a complete or partial application name by which this application can be identified:
Application name
Application NAme
Note: Partial application names are accepted.
Optionally you can provide the following details:
Version Number
1.0
Publisher
Publisher Name
Tell me more ...
< Back
Next >
Cancel

Screenshot 76: Procedura guidata Inventario applicazioni

4. Indicare il nome dell'applicazione. In alternativa, fornire il numero della versione e il nome dell'autore. Fare clic su **Avanti**.

5. Selezionare i profili di scansione che rileveranno l'applicazione non autorizzata (ad es. Scansione completa) e fare clic su **Avanti**.

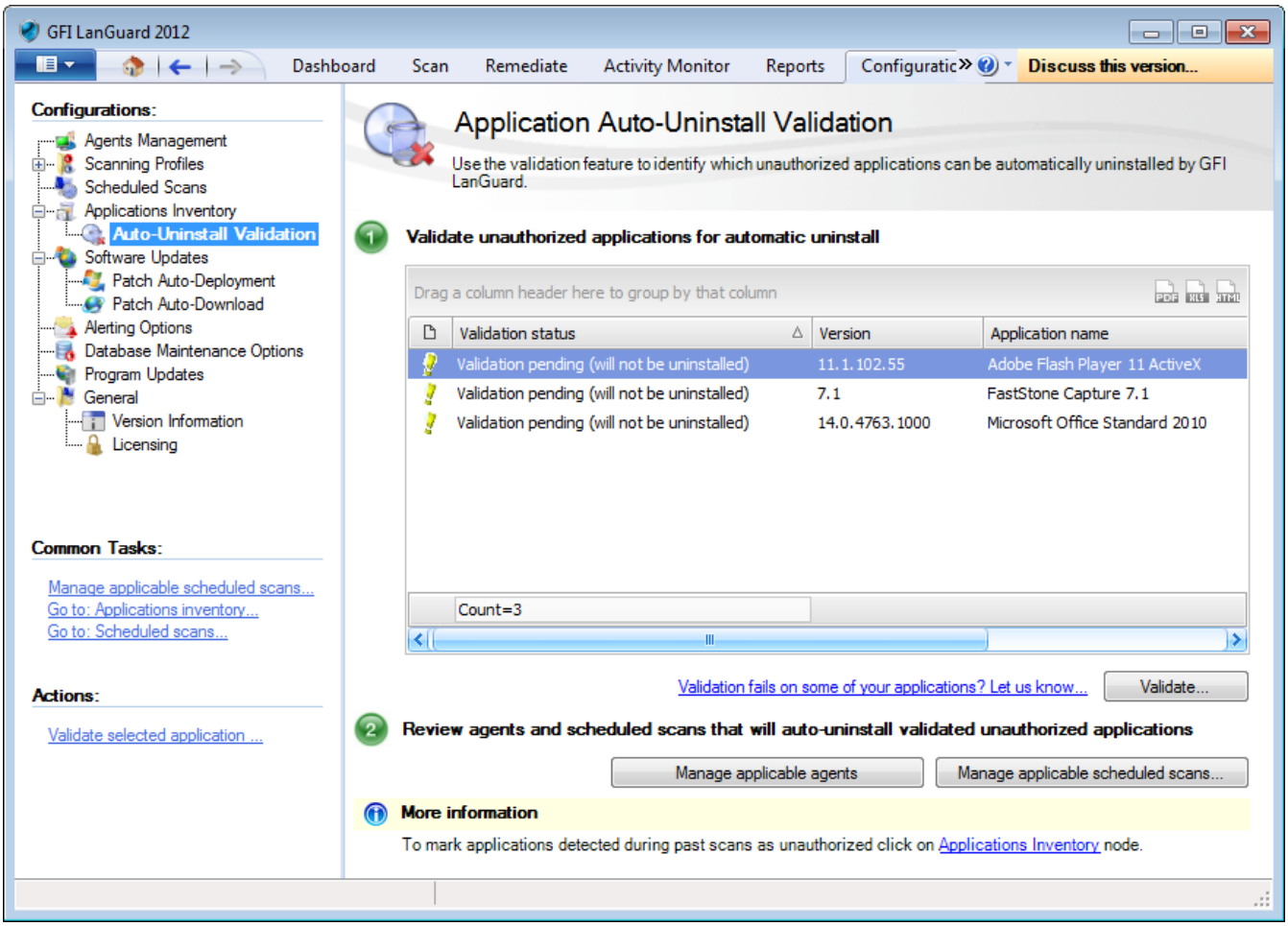
6. Specificare se le modifiche apportate influenzeranno le applicazioni con una corrispondenza del nome completa/parziale. Per continuare, fare clic su **Avanti**.

7. Rivedere le informazioni e fare clic su **Fine**.

Convalida applicazioni non autorizzate per disinstallazione automatica

La convalida della disinstallazione automatica delle applicazioni permette di convalidare il processo di disinstallazione per le applicazioni destinate a essere disinstallate automaticamente da GFI LanGuard. Questo processo deve essere eseguito obbligatoriamente prima del processo di disinstallazione vero e proprio e durante le scansioni non viene disinstallata nessuna applicazione a meno che non sia stata verificata.

1. Fare clic sulla scheda **Configurazione**, selezionare **Inventario applicazioni > Convalida disinstallazione automatica**.



Screenshot 77: Convalida della disinstallazione automatica delle applicazioni

2. Nel riquadro di destra, selezionare un'applicazione da convalidare e fare clic sul pulsante **Convalida**.

3. Nella procedura guidata **Convalida disinstallazione automatica applicazione**, fare clic su **Avanti**.

4. Selezionare il computer sul quale verificare la disinstallazione automatica dell'applicazione e fare clic su **Avanti**.

5. Fornire i dettagli di autenticazione per l'operazione di convalida e fare clic su **Avanti** per continuare.

6. Rivedere le informazioni della procedura guidata Convalida disinstallazione automatica e fare clic su **Avvia**.

Gestione delle scansioni pianificate applicabili

Il pulsante **Gestisci le scansioni pianificate applicabili** consente di revisionare o modificare le scansioni pianificate che eseguiranno l'installazione automatica delle applicazioni convalidate. Per gestire una scansione pianificata:

1. Dal riquadro di convalida **Disinstallazione automatica**, fare clic su **Gestisci scansioni pianificate applicabili**.

2. Dalla finestra di dialogo **Gestisci le scansioni pianificate applicabili**, selezionare una delle opzioni descritte di seguito:

Table 50: Gestione scansioni pianificate applicabili

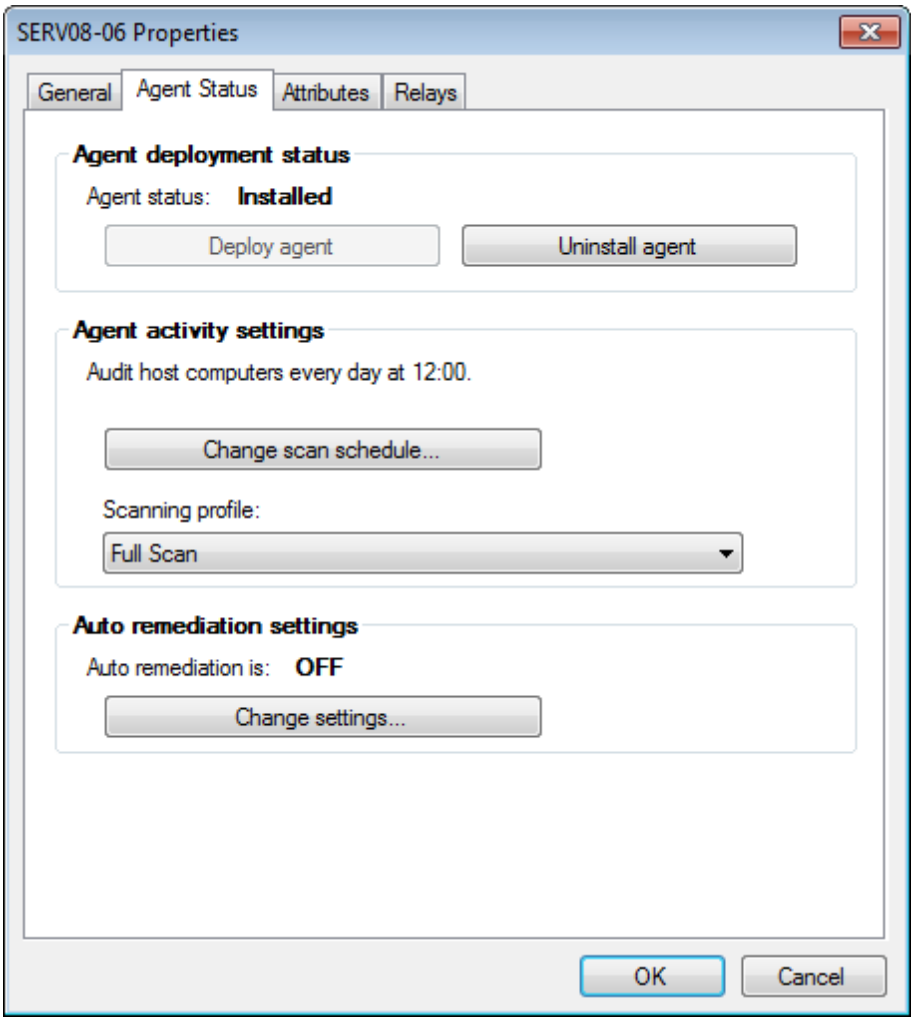
Opzione	Descrizione
Modifica scansione selezionata...	Modifica la scansione pianificata selezionata. For more information, refer to Modifica impostazioni scansione pianificata (page 81).
Crea una nuova scansione pianificata...	Aggiunge una nuova scansione pianificata con la procedura guidata nuova scansione pianificata. For more information, refer to Creazione di una scansione pianificata (page 73).
Visualizza tutte le scansioni pianificate...	Gestisce le scansioni pianificate. For more information, refer to Modifica impostazioni scansione pianificata (page 81).

8.1.4 Configurazione delle opzioni di riparazione automatica

Per modificare le opzioni generali di distribuzione:

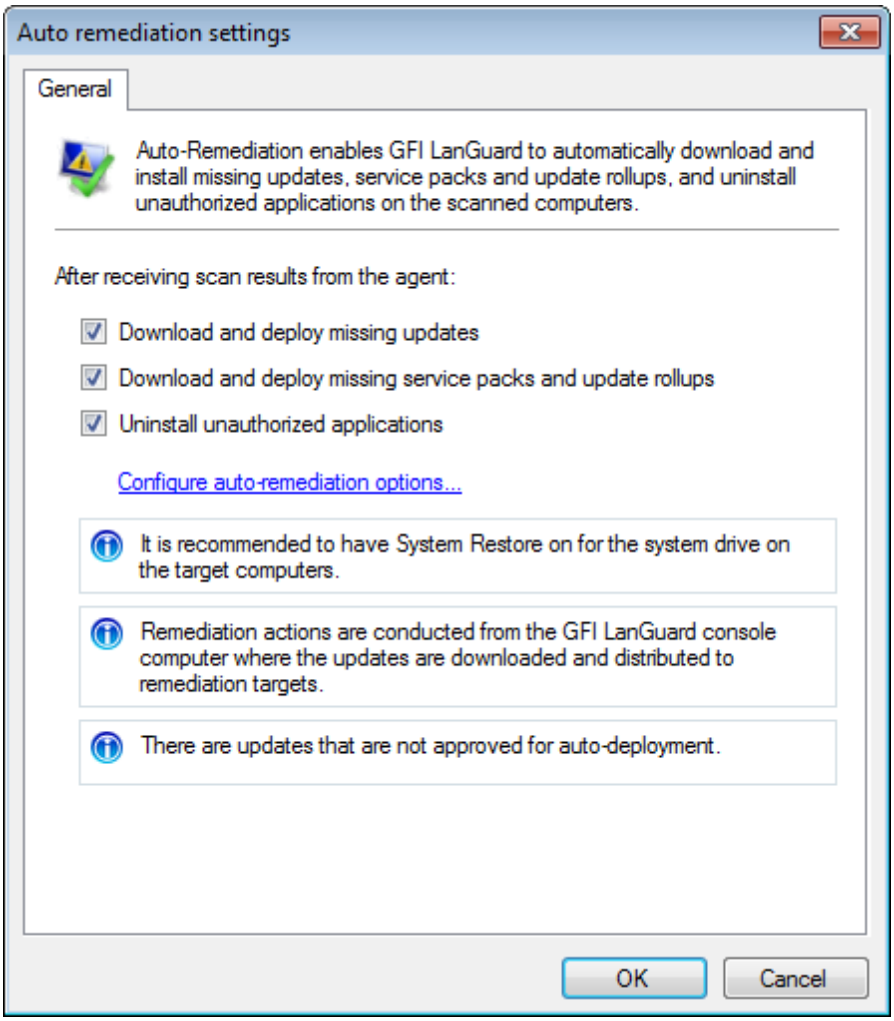
1. Avviare GFI LanGuard.

2. Dalla struttura computer fare clic con il pulsante destro del mouse su un computer/gruppo di computer e selezionare **Proprietà**.



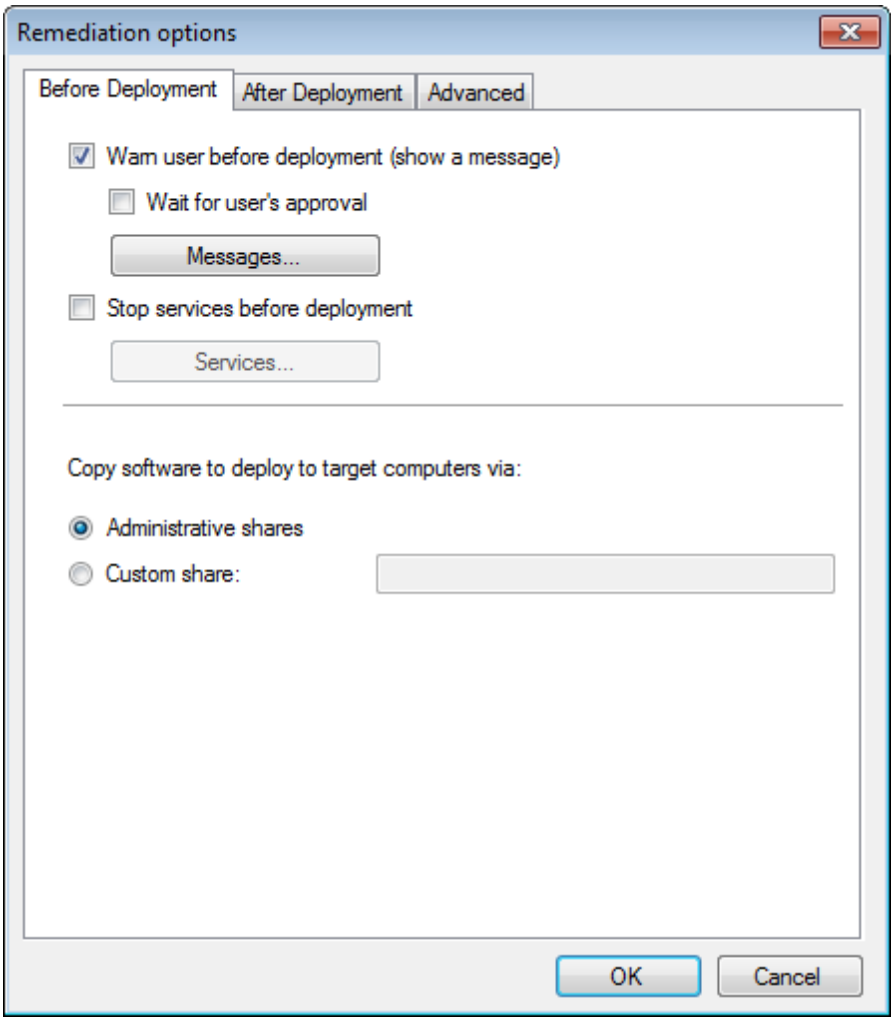
Screenshot 78: Proprietà computer

3. Selezionare la scheda **Stato agente** e da **Impostazioni di riparazione automatica** fare clic su **Cambia impostazioni...**


Auto remediation settings
General
Auto-Remediation enables GFI LanGuard to automatically download and install missing updates, service packs and update rollups, and uninstall unauthorized applications on the scanned computers.
After receiving scan results from the agent:
Download and deploy missing updates
Download and deploy missing service packs and update rollups
Uninstall unauthorized applications
Configure auto-remediation options...
It is recommended to have System Restore on for the system drive on the target computers.
Remediation actions are conducted from the GFI LanGuard console computer where the updates are downloaded and distributed to remediation targets.
There are updates that are not approved for auto-deployment.
OK
Cancel

Screenshot 79: Impostazioni generali di riparazione automatica

4. Selezionare l'azione da eseguire dopo la ricezione dei risultati di scansione dall'agente. Fare clic su **Configura opzioni di riparazione automatica...**

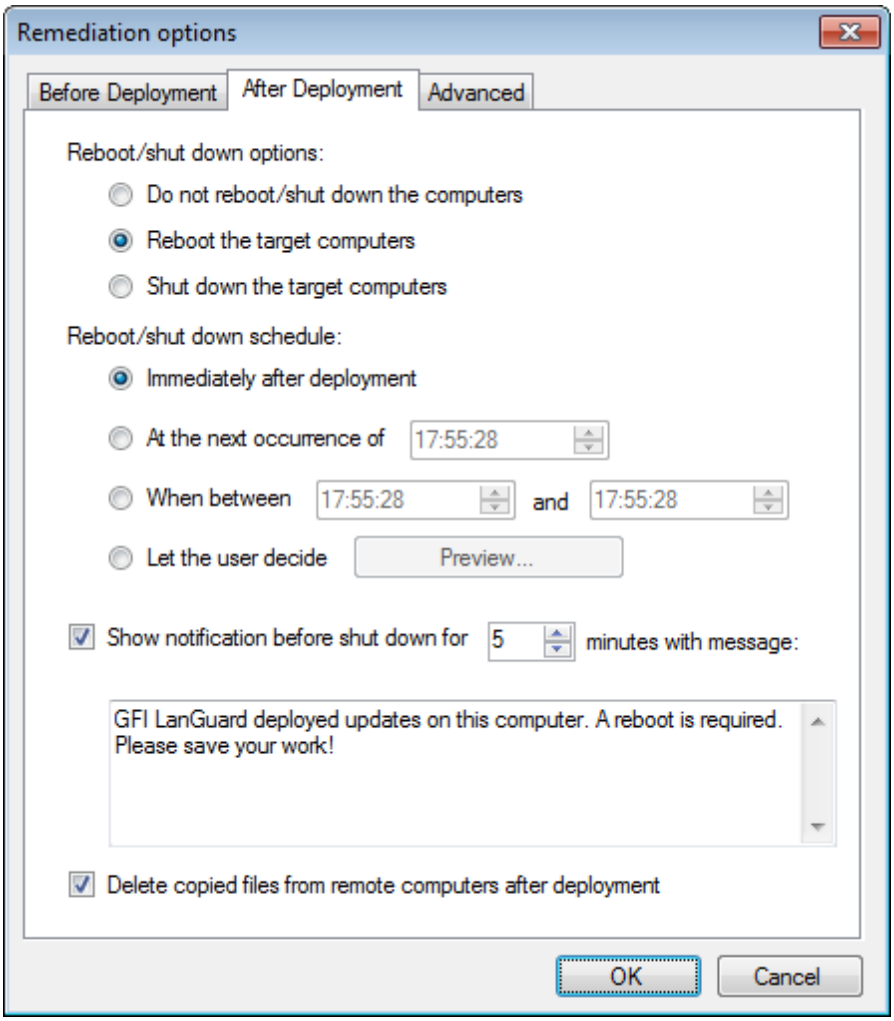


Screenshot 80: Opzioni preliminari alla distribuzione

5. Configurare le opzioni **Prima della distribuzione** descritte di seguito:

Table 51: Prima della distribuzione

Opzione	Descrizione
Attiva i computer non in linea	Se i computer sono disattivati, accenderli. For more information, refer to Configurazione di Wake-on-LAN sulle destinazioni di scansione (page 135).
Avvisa l'utente prima della distribuzione (visualizza un messaggio)	Visualizza un messaggio sul computer di destinazione per avvisare l'utente prima della distribuzione del software.
Attendi approvazione utente	Attendi approvazione utente: attende l'approvazione dell'utente prima della distribuzione del software.
Messaggi	Fare clic su **Messaggi** per selezionare la lingua del computer dell'utente finale e definire il messaggio di avviso. For more information, refer to Configurazione dei messaggi della riparazione automatica (page 137).
Condivisioni amministrative	Esegue una copia del software nelle condivisioni predefinite di rete.
Condivisioni personalizzate	Esegue una copia del software in una condivisione personalizzata. Digitare il nome della cartella nella casella di testo.
Ricorda impostazioni	Salva le impostazioni configurate e le utilizza durante il lavoro di riparazione successivo.



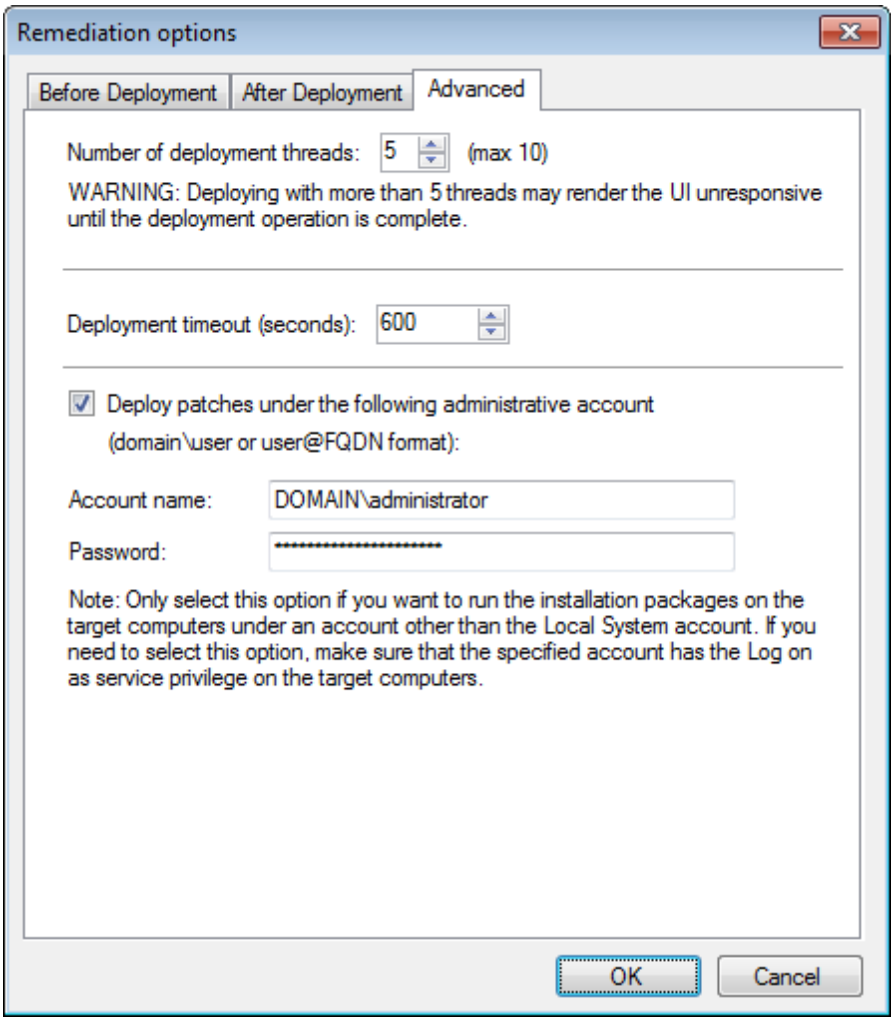
Screenshot 81: Opzioni successive alla distribuzione

6. Fare clic sulla scheda **Dopo la distribuzione**. Configurare le opzioni **Dopo la distribuzione** descritte di seguito:

Table 52: Dopo la distribuzione

Opzione	Descrizione
Non riavviare/arrestare il computer	Selezionare questa opzione per lasciare accesi i computer di destinazione dopo aver risolto le vulnerabilità.
Riavvia i computer di destinazione	Riavvia i computer dopo aver risolto le vulnerabilità.
Arresta i computer di destinazione	Il computer di destinazione si arresterà dopo la distribuzione del software.
Subito dopo la distribuzione	Riavvia/arresta i computer subito dopo aver risolto le vulnerabilità.
Alla prossima occorrenza di	Specifica il momento di riavvio/arresto dei computer.
Se fra	Questa opzione consente di specificare due valori temporali. Se l'operazione di riparazione viene completata tra gli orari specificati, i computer si riavvieranno/arresteranno. Altrimenti, l'operazione di riavvio/arresto verrà posticipata al prossimo ingresso nell'intervallo di tempo specificato.
Lascia decidere all'utente	Per visualizzare una schermata della finestra di dialogo del manuale utente, fare clic su **Anteprima**. Questa finestra di dialogo viene aperta nel computer dell'utente finale dopo aver risolto le vulnerabilità. For more information, refer to Configurazione delle opzioni di riavvio e arresto utente finale (page 137).

Opzione	Descrizione
Mostra notifica prima dell'arresto per	Mostra un messaggio personalizzato nel computer dell'utente finale per il numero di minuti specificato prima del riavvio/dell'arresto.
Elimina file copiati dai computer remoti dopo la distribuzione	Elimina le patch scaricate/i service pack dopo che sono stati distribuiti.
Ricorda impostazioni	Salva le impostazioni configurate e le utilizza durante il lavoro di riparazione successivo.


Remediation options
Before Deployment
After Deployment
Advanced
Number of deployment threads:
5
(max 10)
WARNING: Deploying with more than 5 threads may render the UI unresponsive until the deployment operation is complete.
Deployment timeout (seconds):
600
Deploy patches under the following administrative account
(domain\user or user@FQDN format):
Account name:
DOMAIN\administrator
Password:
Note: Only select this option if you want to run the installation packages on the target computers under an account other than the Local System account. If you need to select this option, make sure that the specified account has the Log on as service privilege on the target computers.
OK
Cancel

Screenshot 82: Opzioni di distribuzione avanzate

7. (Facoltativo) Selezionare la scheda **Avanzate**. Configurare le opzioni descritte di seguito:

Table 53: Opzioni di distribuzione avanzate

Opzione	Descrizione
Numero di thread di distribuzione	Specificare il numero massimo di thread di elaborazione consentiti da avviare quando vengono distribuiti gli aggiornamenti software. Il numero di thread indica il numero di operazioni di distribuzione simultanee gestibili da un agente.
Time-out di distribuzione (secondi)	Specificare il tempo (in secondi) che un agente ha a disposizione per tentare di distribuire un aggiornamento. Se il tempo specificato viene superato, l'agente interrompe la distribuzione senza risposta e avvia un nuovo thread di distribuzione. Questa funzione consente di interrompere il thread del processo: nel caso in cui un aggiornamento impiegasse una quantità di tempo maggiore rispetto a quella prevista normalmente per la distribuzione, l'operazione di riparazione potrà continuare senza compromettere il resto.

Opzione	Descrizione
Distribuisci le patch con il seguente account amministrativo	Selezionare questa opzione per utilizzare un account amministrativo personalizzato per registrare e distribuire le patch nei computer di destinazione. L'account selezionato deve disporre di Accedi come privilegio di servizio nei computer di destinazione. Per ulteriori informazioni sulla configurazione di un account con privilegio di accesso come servizio, fare riferimento a http://go.gfi.com/?pageid=LAN_LogonService.

8. Per applicare le modifiche, fare clic su **OK**.

Configurazione di Wake-on-LAN sulle destinazioni di scansione

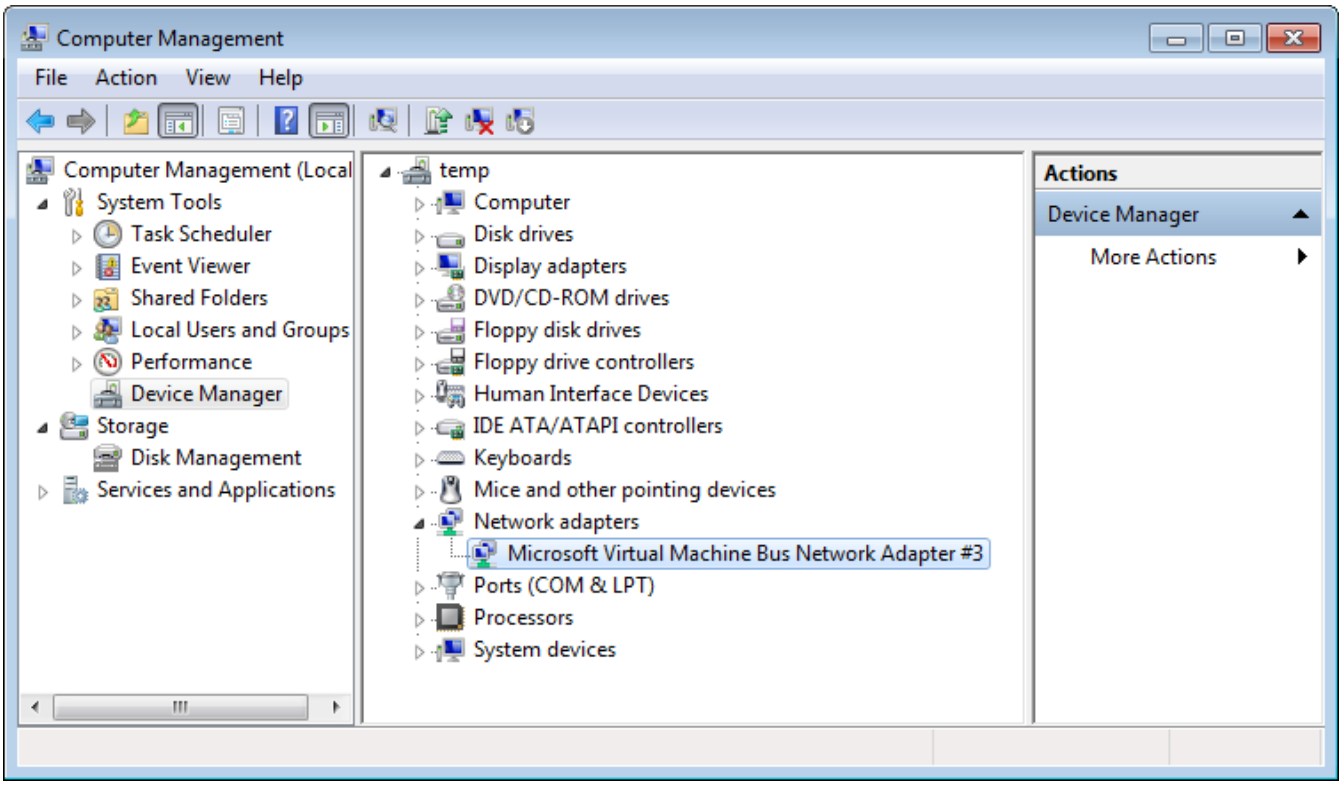
Wake-on-LAN consente a GFI LanGuard di attivare i computer che si trovano nei seguenti stati:

- Arrestato
- Modalità sospensione
- Modalità ibernazione

La scheda madre e la scheda dell'interfaccia di rete del computer che esegue GFI LanGuard devono supportare Wake-on-LAN. Per configurare Wake-on-LAN in Windows® 7:

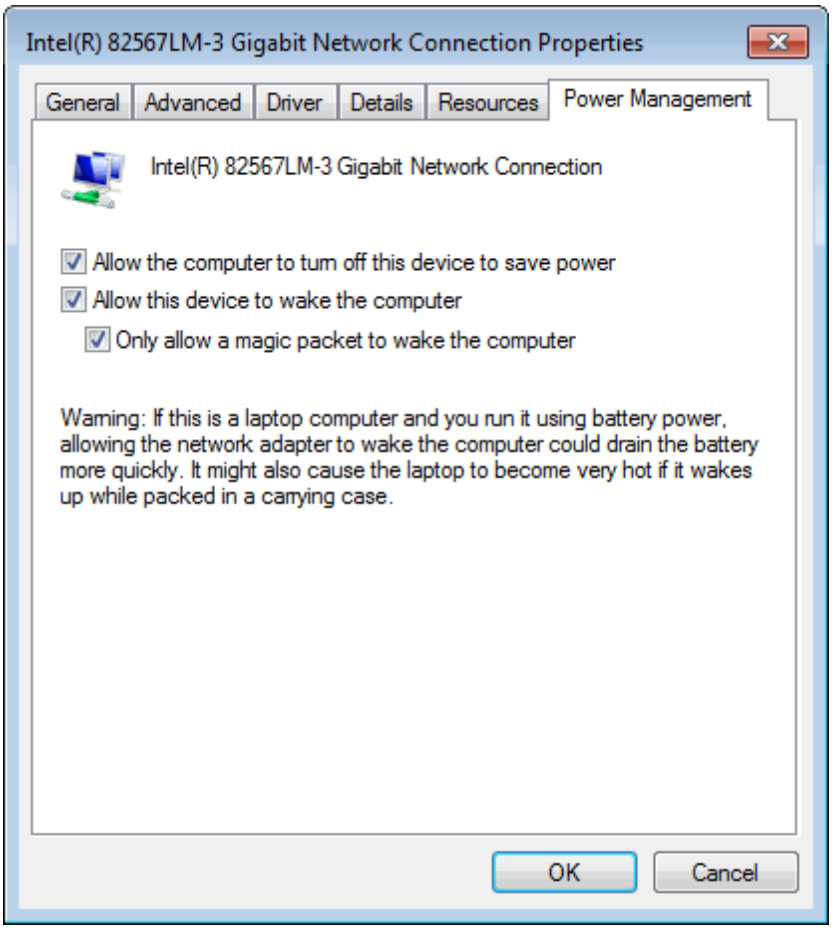
1. Fare clic su **Start**, fare clic con il pulsante destro del mouse su **Computer** e quindi selezionare **Gestione**.

2. Dal pannello di sinistra, espandere **Utilità di sistema** e fare clic su **Gestione dispositivi**.



Screenshot 83: Gestione dispositivi

3. Fare clic con il pulsante destro del mouse sulla **Scheda di rete** e selezionare **Proprietà**.


Intel(R) 82567LM-3 Gigabit Network Connection Properties
General
Advanced
Driver
Details
Resources
Power Management
Intel(R) 82567LM-3 Gigabit Network Connection
Allow the computer to turn off this device to save power
Allow this device to wake the computer
Only allow a magic packet to wake the computer
Warning: If this is a laptop computer and you run it using battery power, allowing the network adapter to wake the computer could drain the battery more quickly. It might also cause the laptop to become very hot if it wakes up while packed in a carrying case.
OK
Cancel

Screenshot 84: Risparmio energia

4. Dalla scheda **Risparmio energia**, selezionare le seguenti opzioni:

- **Consenti al dispositivo di riattivare il computer**
- **Consenti solo a Magic Packet di riattivare il computer**

> **Nota**
>
> **Magic Packet** è il segnale di riattivazione che viene inviato da GFI LanGuard alla scheda di rete della destinazione di scansione.

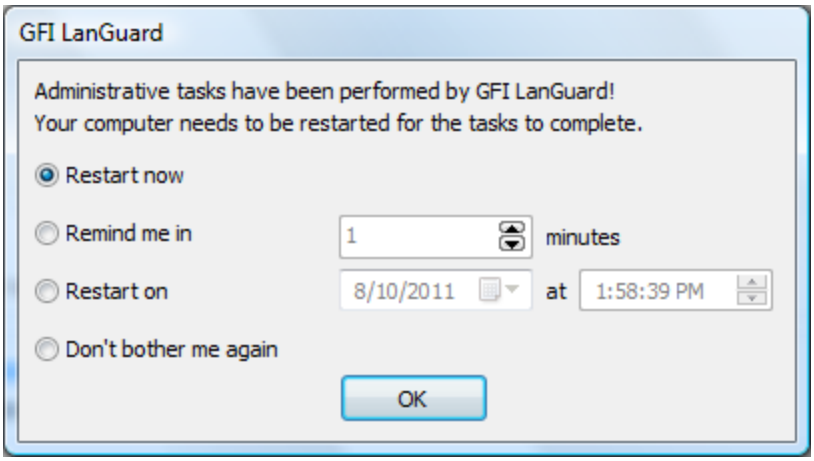
5. Fare clic su **OK**.

Una volta configurata la **scheda di interfaccia di rete**, eseguire una scansione **completa** del computer client. Ciò consente a GFI LanGuard di raccogliere le informazioni necessarie dal computer client. For more information, refer to Scansioni manuali (page 67).

> **IMPORTANTE**
>
> Se tra il computer client e il computer di GFI LanGuard vi sono router, il router e il computer GFI LanGuard devono essere configurati per consentire i pacchetti broadcast Wake-on-LAN sulla porta UDP 9.

8.1.5 Configurazione delle opzioni di riavvio e arresto utente finale

Durante la configurazione delle impostazioni **Dopo la distribuzione**, da **Opzioni di riparazione automatica** è possibile configurare GFI LanGuard affinché notifichi e consenta agli utenti di decidere quando riavviare o arrestare il computer in seguito al completamento di un'attività amministrativa. La finestra di dialogo seguente viene aperta sul computer dell'utente finale e gli consente di selezionare una delle seguenti opzioni:



Screenshot 85: Opzioni di riavvio/arresto

La sottostante tabella illustra le opzioni disponibili:

Table 54: Opzioni di distribuzione avanzate

Opzione	Descrizione
Riavvia adesso	Riavvia/arresta immediatamente il computer dopo il completamento di un'attività amministrativa.
Visualizza tra	Specifica un intervallo di tempo (in minuti) al termine del quale inviare un promemoria all'utente finale.
Riavvia il	Specifica la data e l'ora di riavvio/arresto del computer.
Non visualizzare più	Non viene più inviata alcuna richiesta.

8.1.6 Configurazione dei messaggi della riparazione automatica

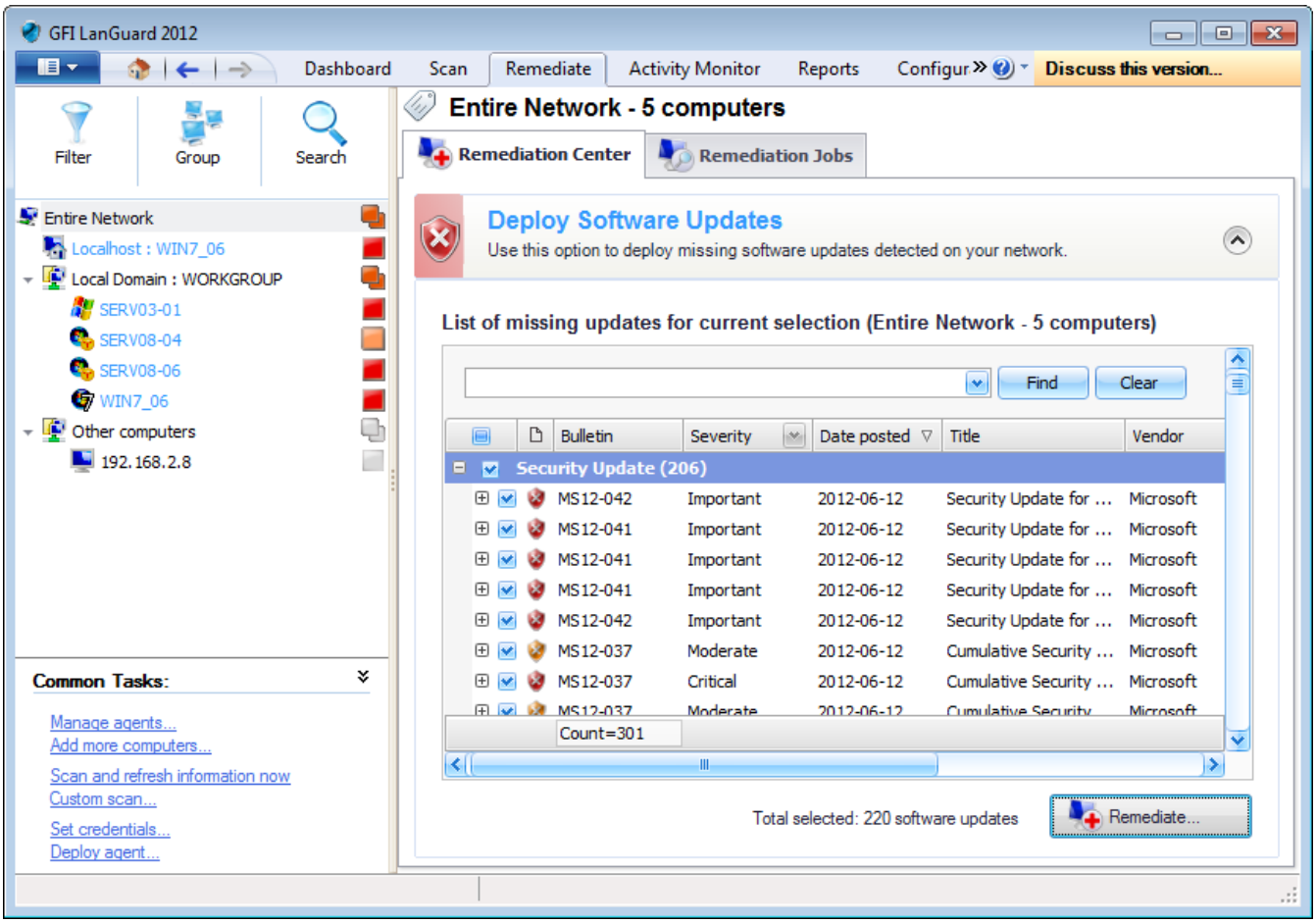
GFI LanGuard consente di visualizzare automaticamente i messaggi di avviso prima e dopo alle operazioni di riparazione. Tali messaggi vengono visualizzati nei computer degli utenti finali e, in alcuni casi, consentono di scegliere le opzioni successive alla distribuzione o di notificarli delle operazioni da effettuare. È possibile personalizzare i messaggi predefiniti e impostare la lingua in base alla lingua del computer di destinazione.

Per configurare i messaggi di avviso:

1. Avviare GFI LanGuard.

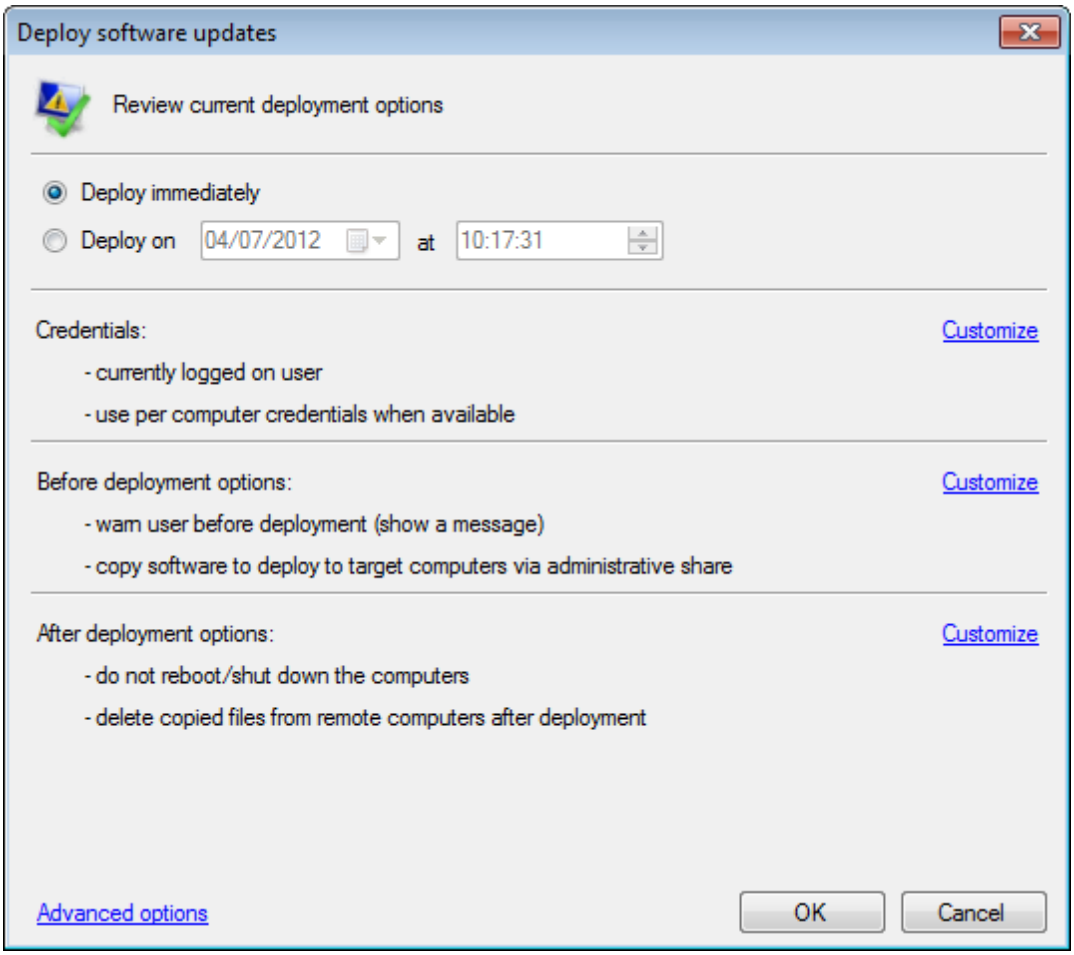
2. Fare clic sulla scheda **Ripara > Centro riparazioni**.

3. Da **Centro riparazioni**, selezionare un'azione di riparazione, come **Distribuisci aggiornamenti software**.



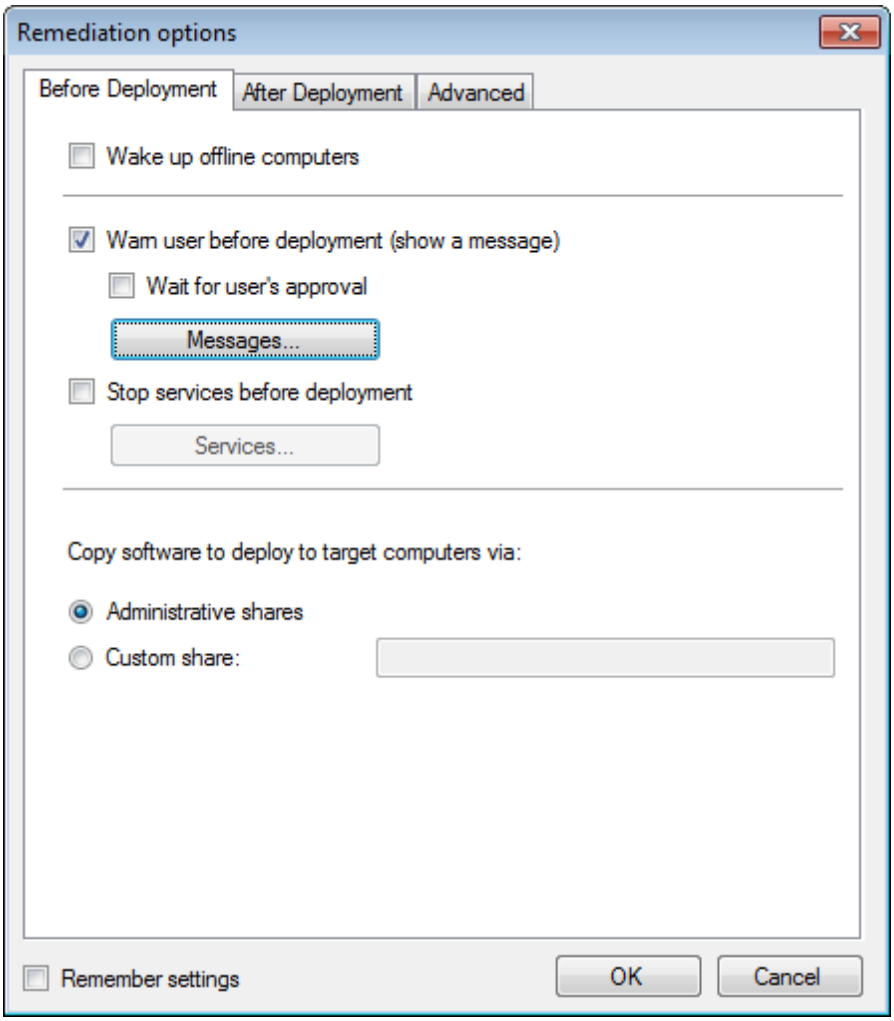
Screenshot 86: Centro riparazioni - Distribuisci aggiornamenti software

4. Fare clic su **Ripara**.



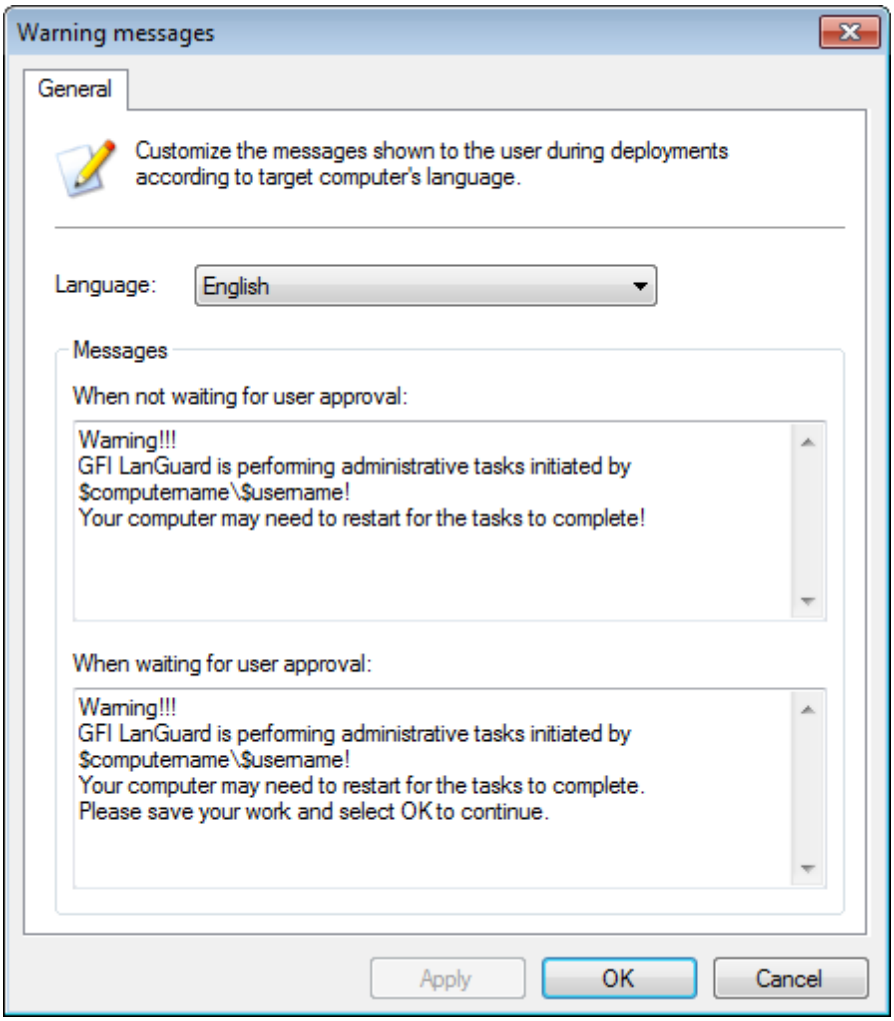
Screenshot 87: Finestra di dialogo Opzioni di distribuzione

5. Fare clic sulla scheda delle **opzioniAvanzate**.



Screenshot 88: Opzioni prima della distribuzione

6. Dalla finestra di dialogo **Opzioni di riparazione**, fare clic sulla scheda **Prima della distribuzione > Messaggi...**.


Warning messages
General
Customize the messages shown to the user during deployments according to target computer's language.
Language:
English
Messages
When not waiting for user approval:
Warning!!!
GFI LanGuard is performing administrative tasks initiated by $computername\$username!
Your computer may need to restart for the tasks to complete!
When waiting for user approval:
Warning!!!
GFI LanGuard is performing administrative tasks initiated by $computername\$username!
Your computer may need to restart for the tasks to complete.
Please save your work and select OK to continue.
Apply
OK
Cancel

Screenshot 89: Personalizzazione messaggi di avviso

7. Personalizzare una delle seguenti opzioni:

Table 55: Messaggi di avviso

Opzione	Descrizione
Lingua	Selezionare la lingua per i messaggi.
Se non in attesa dell'approvazione dell'utente	Utilizzare o personalizzare il messaggio predefinito che viene avviato nel computer dell'utente finale quando GFI LanGuard non è in attesa dell'approvazione.
Se in attesa dell'approvazione dell'utente	Utilizzare o personalizzare il messaggio predefinito che viene avviato nel computer dell'utente finale quando GFI LanGuard è in attesa dell'approvazione.

8. Fare clic su **Applica** e su **OK**.

8.1.7 Configurazione della riparazione automatica agenti

In un ambiente basato su agenti, le opzioni di riparazione automatica possono essere configurate per ciascun agente distribuito. Ciò consente di configurare ciascun agente con opzioni di riparazione automatica specifiche che siano compatibili con i requisiti desiderati.

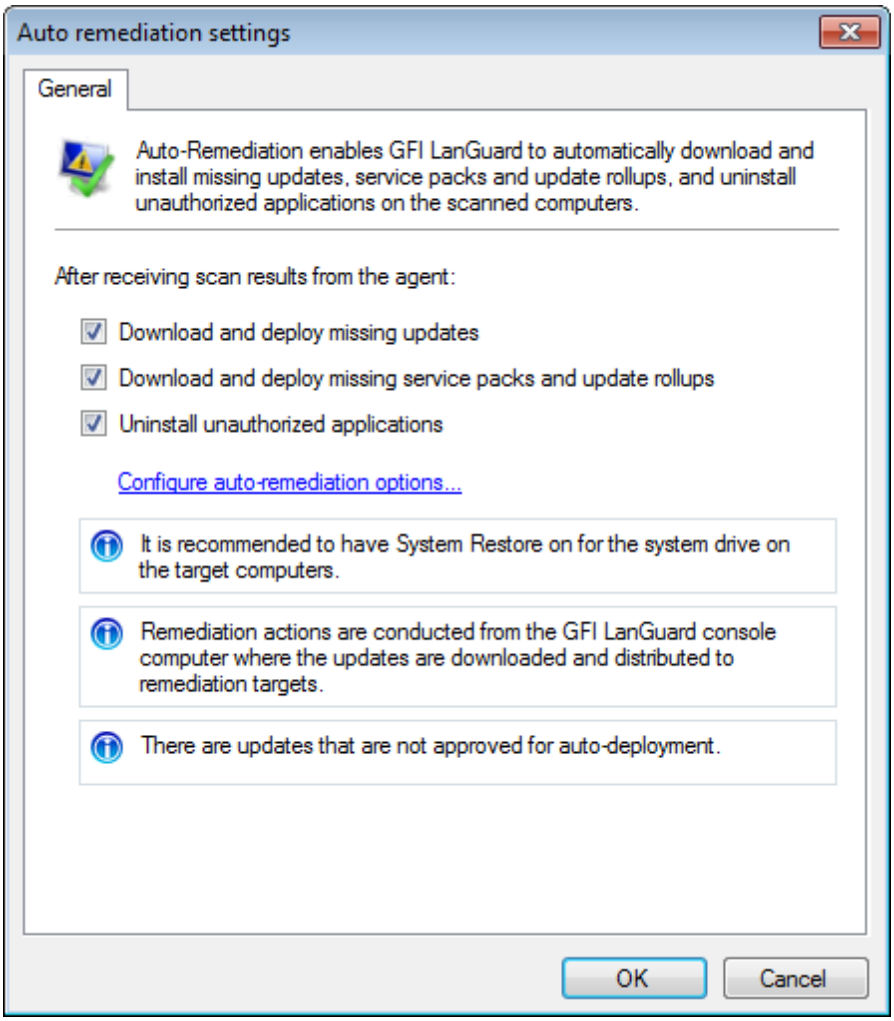
Per configurare le azioni dell'agente di riparazione automatica:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Configurazione> Gestione agenti**.

3. Dal riquadro a destra, fare clic con il pulsante destro del mouse su un agente, quindi selezionare **Proprietà**.

4. Selezionare la scheda **Stato agente** e nella sezione **Impostazioni di riparazione automatica**, fare clic su **Modifica impostazioni**.


Auto remediation settings
General
Auto-Remediation enables GFI LanGuard to automatically download and install missing updates, service packs and update rollups, and uninstall unauthorized applications on the scanned computers.
After receiving scan results from the agent:
Download and deploy missing updates
Download and deploy missing service packs and update rollups
Uninstall unauthorized applications
Configure auto-remediation options...
It is recommended to have System Restore on for the system drive on the target computers.
Remediation actions are conducted from the GFI LanGuard console computer where the updates are downloaded and distributed to remediation targets.
There are updates that are not approved for auto-deployment.
OK
Cancel

Screenshot 90: Riparazione automatica agente

5. Selezionare **Download e distribuzione degli aggiornamenti mancanti** per abilitare la riparazione automatica delle patch mancanti.

6. Selezionare **Download e distribuzione dei service pack e degli aggiornamenti cumulativi mancanti** per abilitare la riparazione automatica dei service pack mancanti.

7. Selezionare **Disinstallazione applicazioni non autorizzate** per abilitare la riparazione automatica delle applicazioni non autorizzate.

8. (Facoltativo) Fare clic su **Configura opzioni per la riparazione automatica…** per personalizzare ulteriormente le opzioni di riparazione. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130)..

9. Fare clic su **OK**.

8.2 Riparazione manuale

Oltre a scaricare automaticamente le patch e i service pack, GFI LanGuard può anche distribuire questi aggiornamenti su tutta la rete e richiamare tutte le patch distribuite.

Le operazioni di distribuzione e ripristino delle patch sono gestite da un servizio agente che si occupa di tutti i trasferimenti di file tra GFI LanGuard e le destinazioni remote. Questo servizio viene installato automaticamente sul computer di destinazione remoto durante il processo di distribuzione della patch

Attività di riparazione manuale:

- Rivedere le note importanti sulla Riparazione manuale
- Ulteriori informazioni sul Centro riparazioni
- Distribuisci aggiornamenti software
- Disinstalla aggiornamenti software
- Distribuzione software personalizzato
- Disinstalla applicazioni
- Protezione dal malware
- Connessione in remoto a un computer tramite GFI LanGuard

8.2.1 Note sulla riparazione manuale

1. Anche se ciò avviene di rado, le patch vengono solitamente richiamate in seguito alla scoperta di nuove vulnerabilità provocate dall'installazione di questi aggiornamenti, come nel caso di problemi di conflitto con il software o l'hardware presenti. Alcuni esempi di aggiornamenti richiamati dal produttore comprendono le patch MS03-045 e MS03-047 per Exchange rilasciate da Microsoft® il 15 ottobre 2006.

2. Assicurarsi che il servizio NetBIOS sia abilitato sul computer di destinazione remoto. For more information, refer to Configurazione di NetBIOS (page 252).

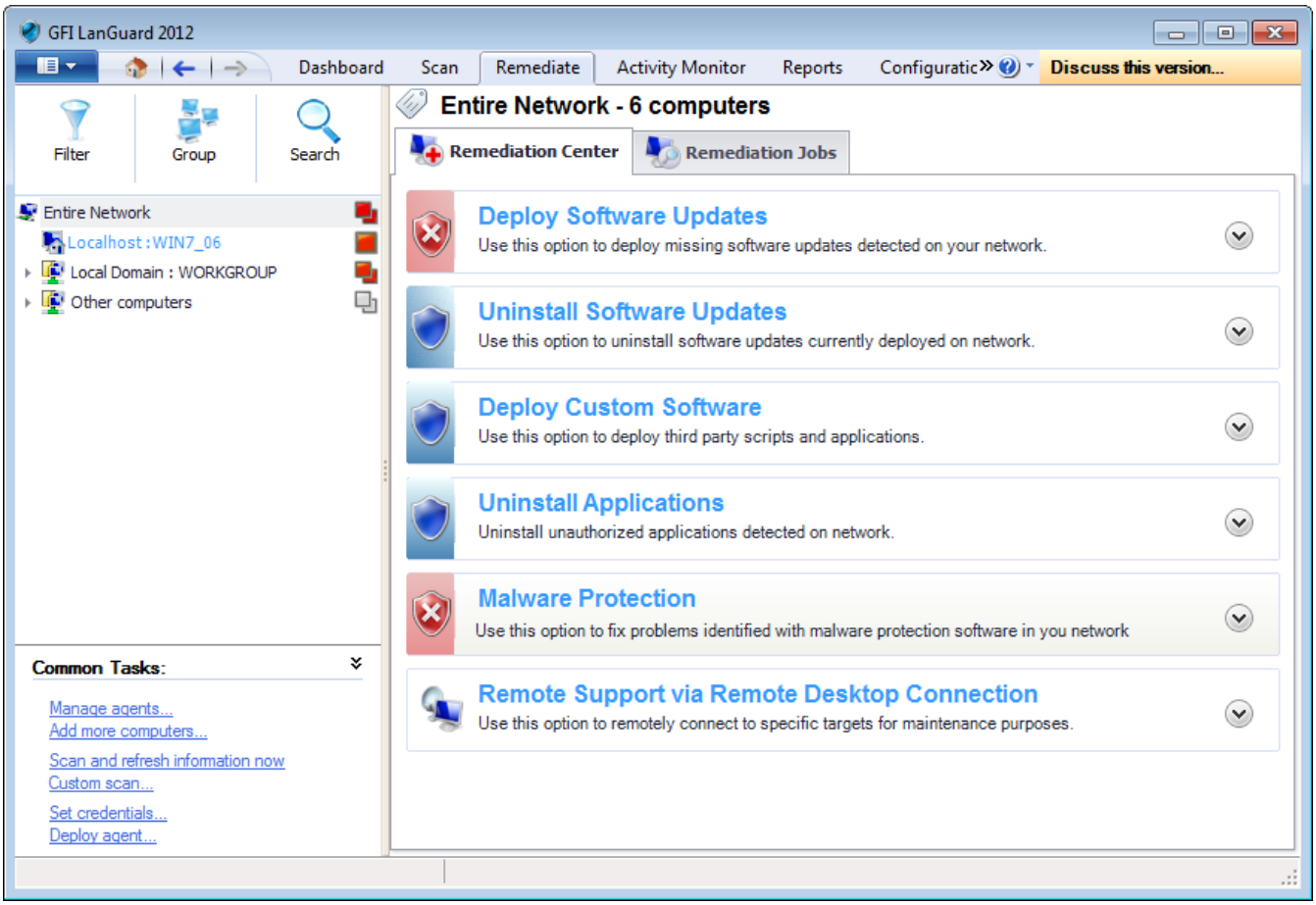
3. Un elenco completo di prodotti Microsoft per i quali GFI LanGuard è in grado di scaricare e distribuire le patch è disponibile all'indirizzo http://go.gfi.com/?pageid=ms_app_fullreport

4. Le patch di aggiornamenti software diversi da Microsoft che sono supportate da GFI LanGuard sono disponibili all'indirizzo http://go.gfi.com/?pageid=3p_fullreport

5. GFI LanGuard può essere configurato in modo da scaricare automaticamente le patch e i service pack mancanti scoperti durante una scansione di sicurezza di rete. For more information, refer to Configurazione della distribuzione automatica degli aggiornamenti mancanti (page 121).

8.2.2 Utilizzo del Centro riparazioni

Il **Centro riparazioni** consente di risolvere i problemi di sicurezza individuati durante una scansione di rete tramite la distribuzione o la disinstallazione delle applicazioni dai computer di destinazione. Per accedere al **Centro riparazioni**, selezionare la scheda **Ripara>Centro riparazioni**.



Screenshot 91: Centro riparazioni

Dal pannello a sinistra, espandere e individuare un computer o dominio in cui eseguire le operazioni di riparazione. Le opzioni di riparazione disponibili sono descritte di seguito:

Table 56: Azioni di riparazione

Azione	Descrizione
Distribuisci aggiornamenti software	Distribuisce le patch mancanti rilevate durante il controllo dei computer di destinazione. For more information, refer to Distribuzione aggiornamenti software (page 144).
Disinstalla aggiornamenti software	Disinstalla i service pack dai computer di destinazione. For more information, refer to Disinstallazione aggiornamenti software (page 147).
Distribuisci software personalizzato	Distribuisce le applicazioni e gli script personalizzati nei computer di destinazione. For more information, refer to Distribuzione software personalizzato (page 149).
Disinstalla applicazioni	Disinstalla le applicazioni dai computer di destinazione. For more information, refer to Disinstallazione delle applicazioni personalizzate (page 151).
Protezione antimalware	Esegue operazioni antimalware sui computer di destinazione. For more information, refer to Protezione antimalware (page 152).
Supporto remoto tramite connessione desktop remoto	Connessione a un computer di destinazione ed esecuzione di attività amministrative tramite la connessione desktop remoto. For more information, refer to Utilizzo del supporto del desktop remoto (page 154).

8.2.3 Distribuzione aggiornamenti software

Utilizzare la funzione **Distribuisci aggiornamenti software** per la distribuzione manuale di:

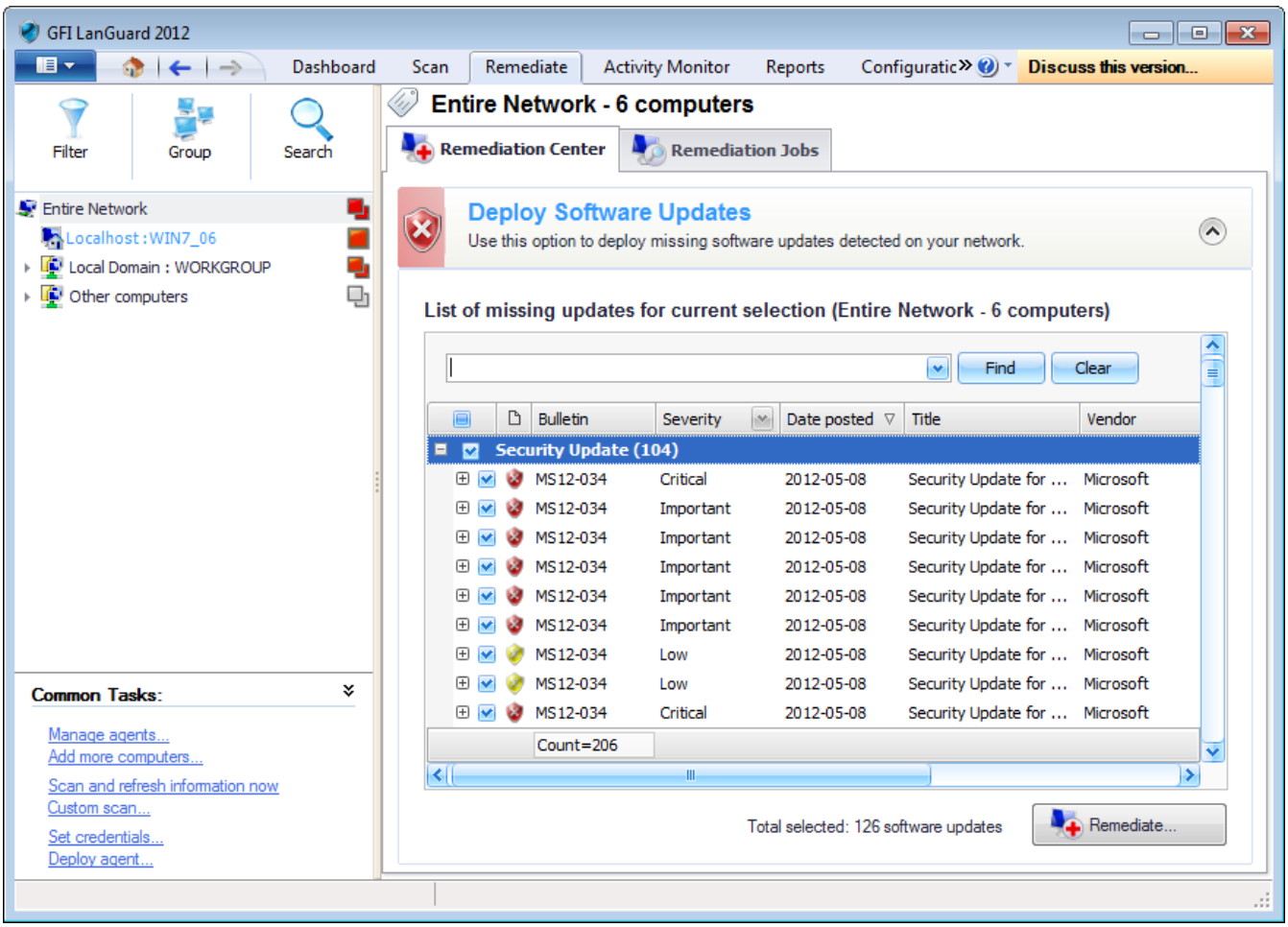
- Service pack e aggiornamenti cumulativi mancanti
- Aggiornamenti di sicurezza mancanti
- Aggiornamenti non di sicurezza mancanti.

Questa funzione consente di selezionare gli elementi che si desidera distribuire e fornisce una descrizione dettagliata di ciascuno.

> **Nota**
>
> Per visualizzare informazioni aggiuntive su un aggiornamento, fare clic con il pulsante destro del mouse su un aggiornamento, quindi selezionare **Ulteriori dettagli > Info bollettino...**

Per distribuire manualmente gli aggiornamenti software:

1. Avviare GFI LanGuard.
2. Fare clic sulla scheda **Ripara** ed espandere **Distribuisci aggiornamenti software**.



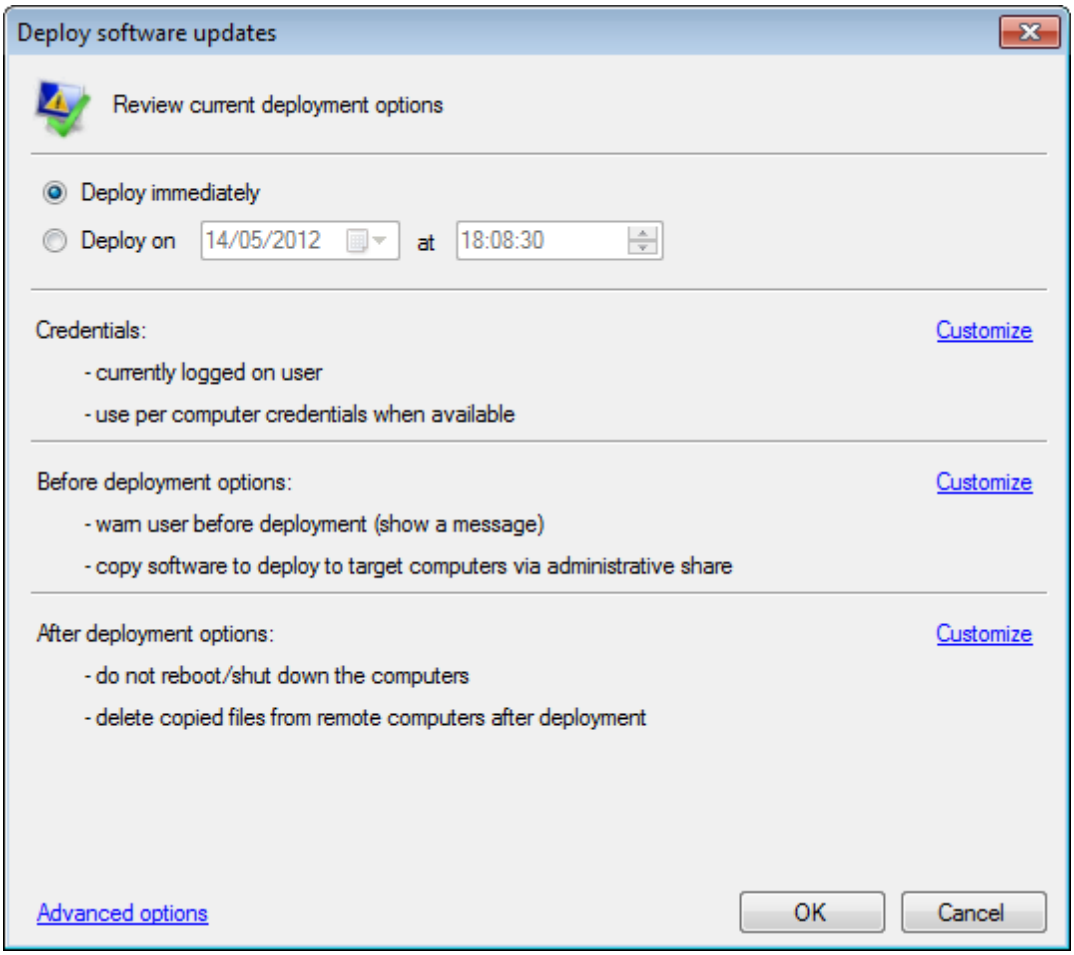
Screenshot 92: Distribuzione aggiornamenti software

3. Dalla struttura computer selezionare il computer/gruppo in cui distribuire gli aggiornamenti software.
4. Da **Elenco degli aggiornamenti mancanti** selezionare gli aggiornamenti da distribuire.

Nota

Utilizzare la barra della ricerca per cercare gli aggiornamenti specifici mancanti o utilizzare le opzioni di filtro per ciascuna intestazione di colonna così da visualizzare soltanto i dati necessari.

5. Fare clic su **Ripara**.



Screenshot 93: Opzioni di Distribuisci aggiornamenti software

6. La finestra di dialogo **Distribuisci aggiornamenti software** consente di modificare le opzioni di distribuzione prima di avviare l'operazione di distribuzione. Rivedere le opzioni descritte di seguito:

Table 57: Opzioni di Distribuisci aggiornamenti software

Opzione	Descrizione
Distribuisci immediatamente	Selezionata per impostazione predefinita. Lasciare l'opzione selezionata per la distribuzione immediata degli aggiornamenti mancanti.
Distribuisci il	Specificare la data e l'orario per la distribuzione degli aggiornamenti mancanti.
Credenziali	Fornisce le impostazioni delle credenziali per gli aggiornamenti. Per modificare le impostazioni, fare clic su **Personalizza**.
Opzioni preliminari alla distribuzione	Fornisce le azioni eseguite prima di distribuire gli aggiornamenti software. Fare clic su **Personalizza** per modificare il messaggio prima della distribuzione e il tipo di condivisione creata per trasferire gli aggiornamenti e i file dei dettagli di scansione.
Opzioni successive alla distribuzione	Fornisce le azioni eseguite dopo la distribuzione degli aggiornamenti software mancanti. Fare clic su **Personalizza** per configurare il riavvio o l'arresto dei computer oppure la visualizzazione di un messaggio all'utente finale.

Opzione	Descrizione
Opzioni avanzate	Fare clic su **Opzioni avanzate** per configurare: » il numero di thread di distribuzione. Massimo = 10 » Time-out di distribuzione » Credenziali alternative. Selezionare **Ricorda impostazioni** per riutilizzare la stessa configurazione quando si esegue il processo di distribuzione successivo. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130)..

7. Fare clic su **OK** per avviare la distribuzione degli aggiornamenti. Si viene indirizzati automaticamente alla scheda **Operazioni di riparazione** che consente di monitorare l'avanzamento dell'operazione di distribuzione.

8.2.4 Disinstallazione aggiornamenti software

La funzione **Disinstalla aggiornamenti software** consente di rimuovere manualmente quanto segue:

» Service pack e aggiornamenti cumulativi installati

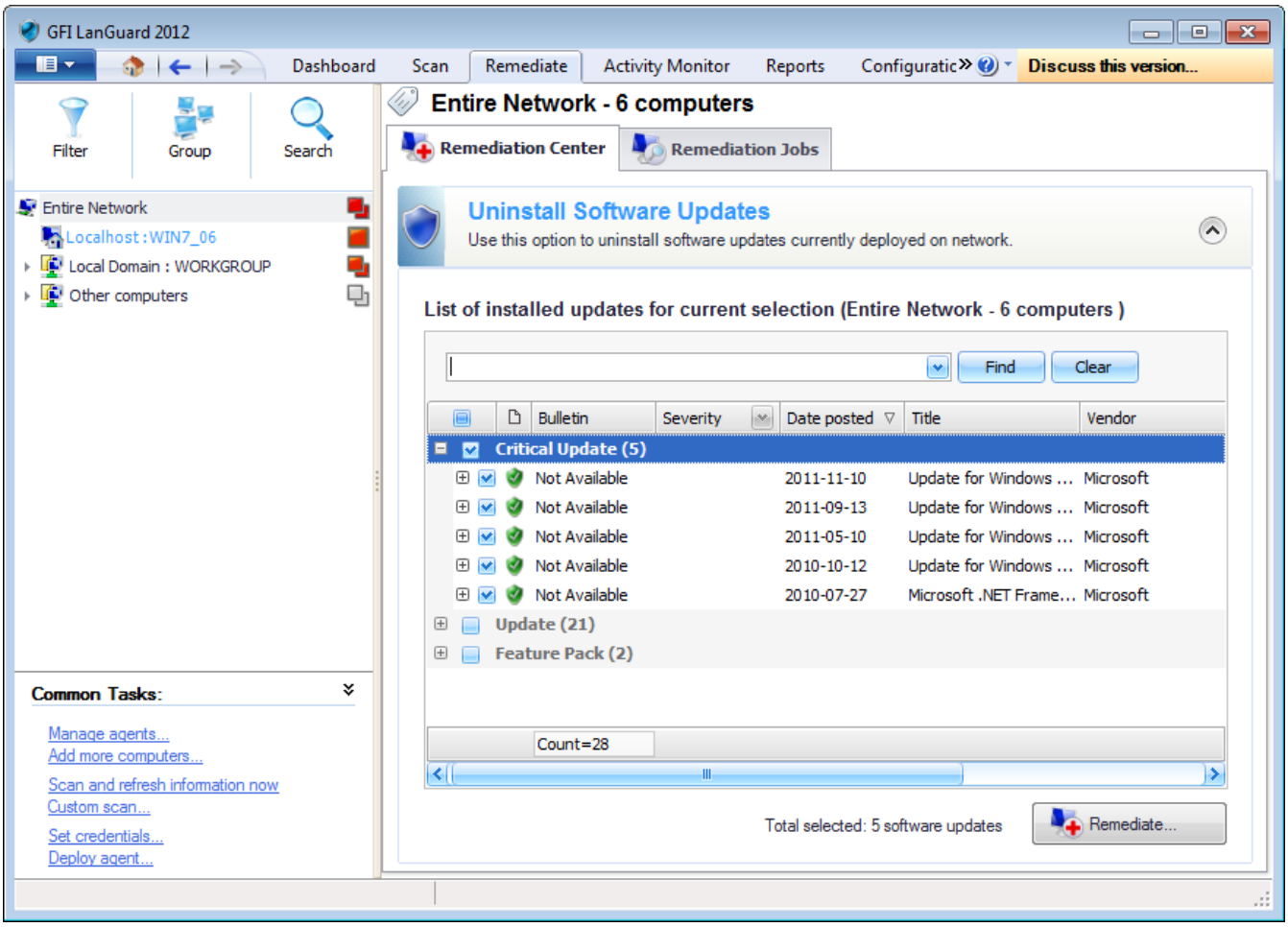
» Aggiornamenti di sicurezza installati

» Aggiornamenti non di sicurezza installati.

Per disinstallare manualmente gli aggiornamenti software:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Ripara** ed espandere **Disinstalla aggiornamenti software**.



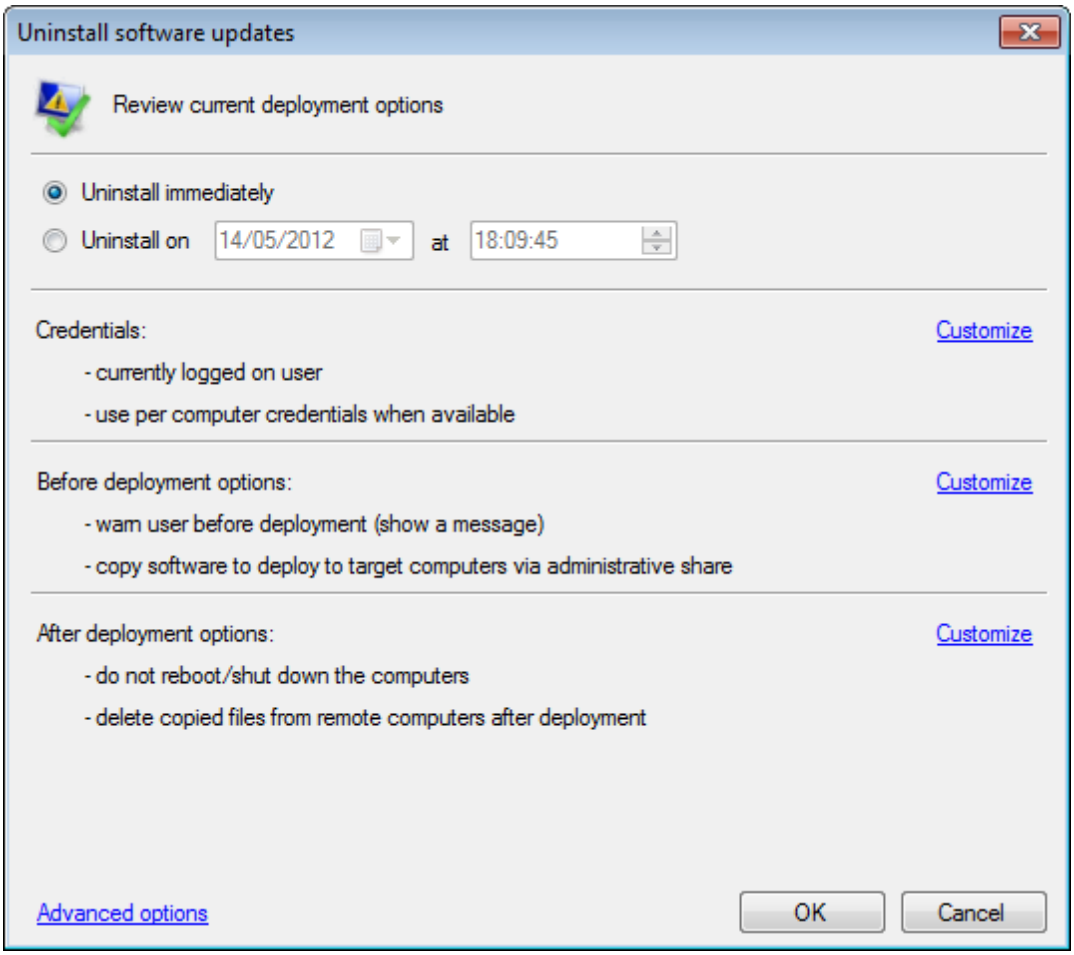
Screenshot 94: Disinstallazione aggiornamenti software

3. Dalla struttura computer selezionare il computer/gruppo da cui disinstallare gli aggiornamenti software.

4. Dall'**elenco degli aggiornamenti installati** selezionare gli aggiornamenti che si desidera disinstallare.

> **Nota**
>
> Utilizzare la barra della ricerca per cercare gli aggiornamenti specifici installati o utilizzare le opzioni di filtro per ciascuna intestazione di colonna così da visualizzare soltanto i dati necessari.

5. Fare clic su **Ripara**.



Screenshot 95: Opzioni di Disinstalla aggiornamenti software

6. La finestra di dialogo **Disinstalla aggiornamenti software** consente di modificare le opzioni di disinstallazione prima di avviare l'operazione di disinstallazione. Rivedere le opzioni descritte di seguito:

Table 58: Opzioni di Disinstalla aggiornamenti software

Opzione	Descrizione
Disinstalla immediatamente	Selezionata per impostazione predefinita. Lasciare l'opzione selezionata se si desidera disinstallare immediatamente gli aggiornamenti.
disinstalla il	Specificare la data e l'orario per la disinstallazione degli aggiornamenti.

Opzione	Descrizione
Credenziali	Fornisce le impostazioni delle credenziali utilizzate per la disinstallazione degli aggiornamenti. Per modificare le impostazioni e utilizzare le credenziali alternative, fare clic su **Personalizza**.
Opzioni preliminari alla distribuzione	Fornisce le azioni eseguite prima di disinstallare gli aggiornamenti software. Fare clic su **Personalizza** per modificare il messaggio prima della distribuzione e la modalità delle condivisioni utilizzata per trasferire gli aggiornamenti.
Opzioni successive alla distribuzione	Fornisce le azioni eseguite dopo la disinstallazione degli aggiornamenti software. Fare clic su **Personalizza** per configurare il riavvio o l'arresto dei computer oppure la visualizzazione di un messaggio all'utente finale.
Opzioni avanzate	Fare clic su **Opzioni avanzate** per configurare: » il numero di thread di distribuzione. Massimo = 10 » Time-out di distribuzione » Credenziali alternative. Selezionare **Ricorda impostazioni** per riutilizzarle quando è in esecuzione l'operazione di distribuzione successiva. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130)..

7. Fare clic su **OK** per avviare la disinstallazione degli aggiornamenti selezionati. Si viene indirizzati automaticamente alla scheda **Operazioni di riparazione** che consente di monitorare l'avanzamento dell'operazione di disinstallazione.

8.2.5 Distribuzione software personalizzato

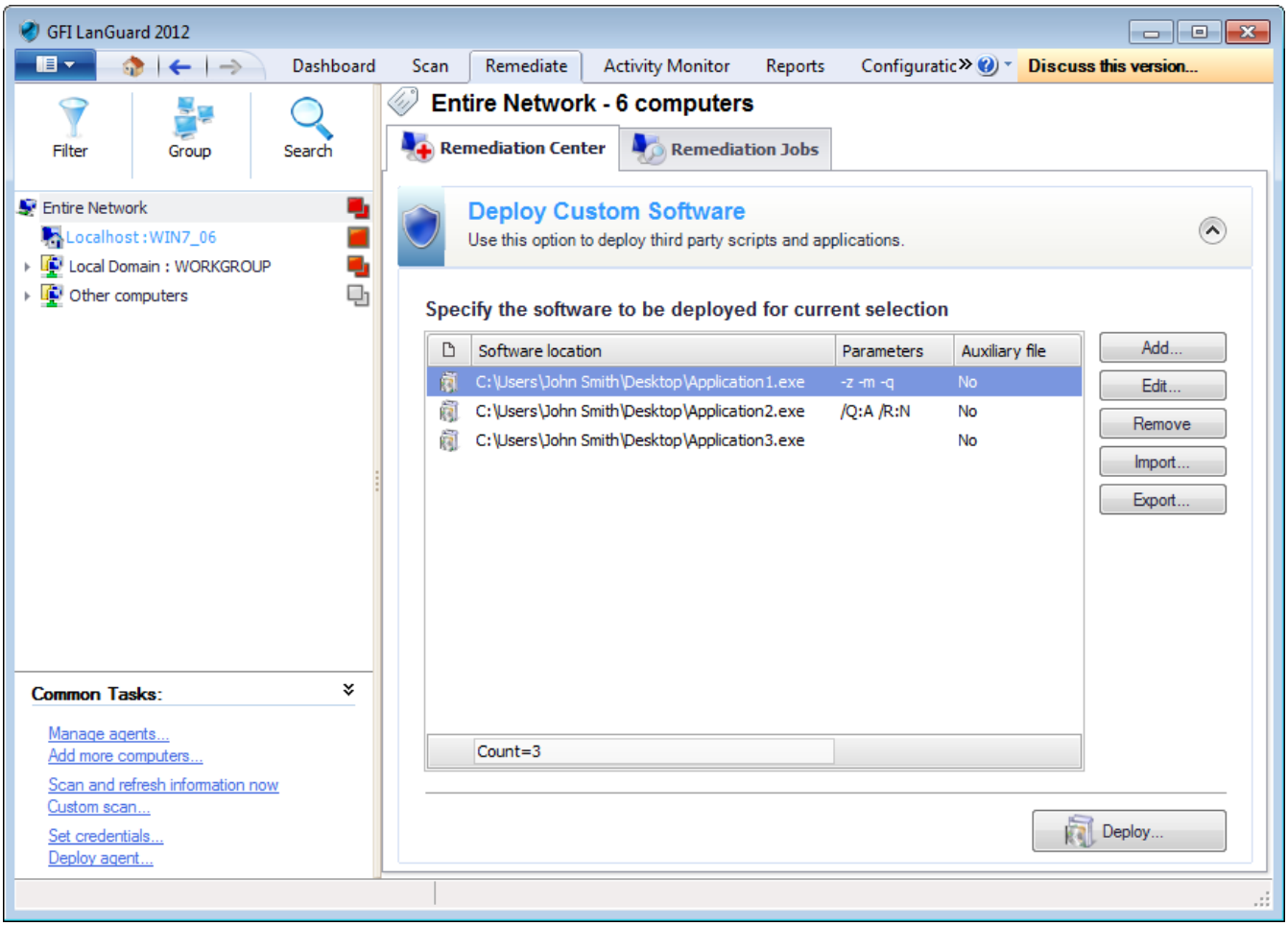
In aggiunta agli aggiornamenti di sicurezza e alle patch, GFI LanGuard consente anche di distribuire in remoto software personalizzato o di terze parti su tutta la rete. I software che possono essere distribuiti in remoto comprendono:

- Applicazioni di sicurezza come soluzioni antivirus/antispyware e software firewall
- Aggiornamenti e patch per software di terze parti come aggiornamenti di firme antivirus/antispyware
- Codice personalizzato come script e file batch
- Applicazioni desktop come Microsoft® Office 2007 e altro.

Per specificare il software da distribuire:

1. Fare clic sulla scheda **Ripara> Centro riparazioni**.

2. Dalla struttura computer, selezionare i computer dove verrà distribuito il nuovo software e fare clic su **Distribuisci software personalizzato**.



Screenshot 96: Elenco di software da distribuire

3. Utilizzare le opzioni descritte di seguito per aggiungere le applicazioni da distribuire:

Table 59: Opzioni disponibili in Distribuisci software personalizzato

Opzione	Descrizione
Aggiungi	Per avviare la finestra di dialogo Aggiungi software personalizzato, selezionare questo pulsante. La finestra consente di aggiungere un'applicazione all'elenco ed eventualmente configurarne i parametri.
Modifica	Selezionare un'applicazione e fare clic su questo pulsante per avviare la finestra di dialogo Aggiungi software personalizzato. Questa finestra di dialogo consente di modificare i parametri di installazione esistenti.
Rimuovi	Selezionare un'applicazione dall'elenco e fare clic su questo pulsante per rimuoverla.
Importa	Selezionare questo pulsante per importare i parametri delle applicazioni da un file XML.
Esporta	Selezionare questo pulsante per esportare i parametri delle applicazioni in un file XML.

4. Fare clic su **Distribuisci** e configurare le opzioni descritte di seguito:

Table 60: Opzioni di distribuzione

Opzione	Descrizione
Distribuisci immediatamente	Distribuisce immediatamente le applicazioni selezionate.
Distribuisci il	Distribuisce le applicazioni selezionate a una data e ora specifiche. Configurare quando distribuire le applicazioni.
Credenziali	Selezionare il metodo di autenticazione da utilizzare o specificare un nome utente e una password. Selezionare **Utilizza credenziali computer se disponibili** per utilizzare le credenziali specificate nelle proprietà del computer. For more information, refer to Proprietà agente (page 49).

Opzione	Descrizione
Opzioni preliminari alla distribuzione	Configurare le azioni da effettuare prima di distribuire le applicazioni selezionate. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).
Opzioni successive alla distribuzione	Configurare le azioni da effettuare dopo la distribuzione delle applicazioni selezionate. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).
Opzioni avanzate	Configurare altre opzioni relative al riavvio/arresto ed eliminare i file copiati dai computer remoti. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).

5. Fare clic su **OK**.

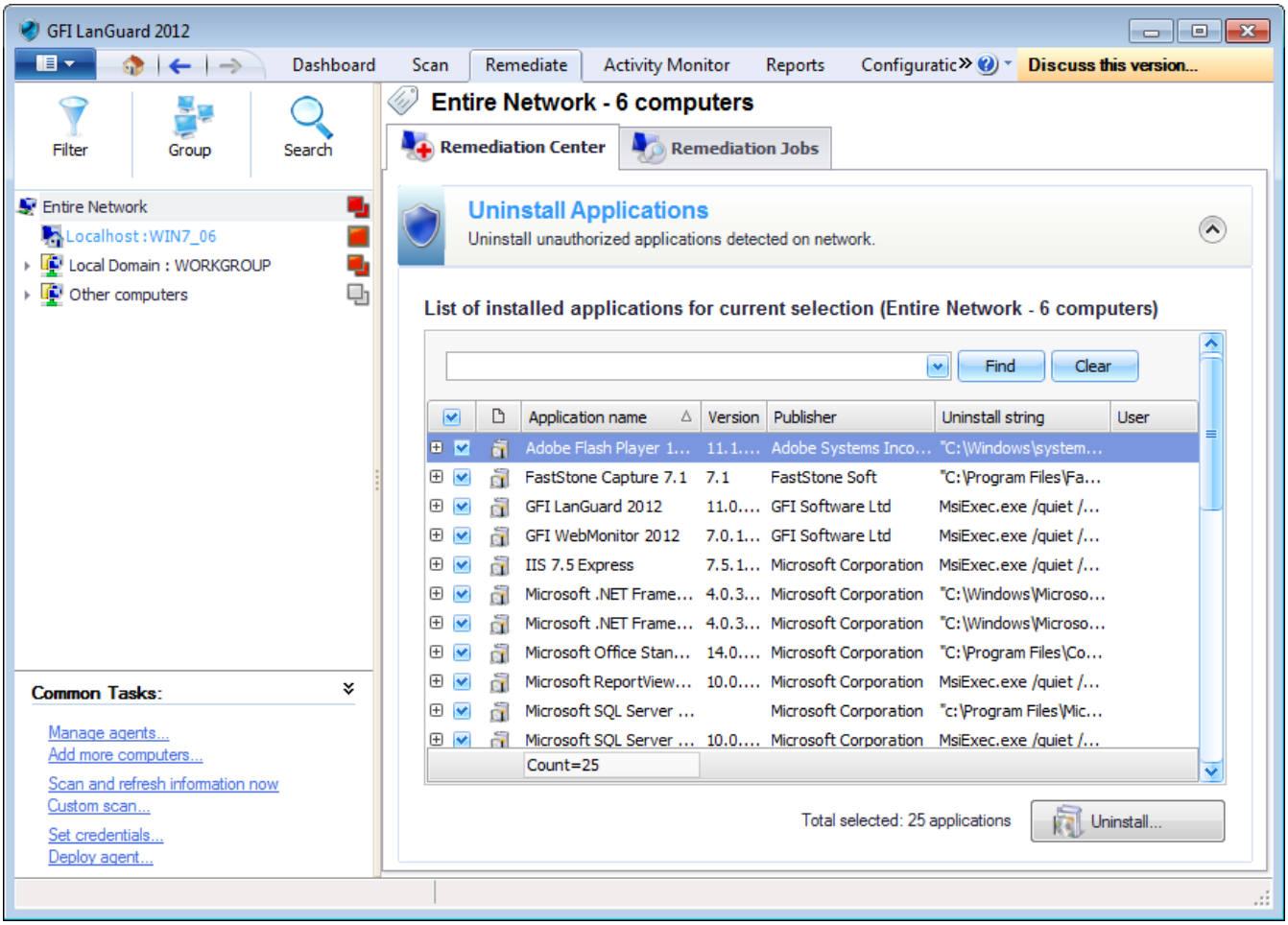
6. Per visualizzare l'avanzamento della distribuzione, fare clic su **Operazioni di riparazione** nel pannello a destra.

8.2.6 Disinstallazione delle applicazioni personalizzate

Tramite questa funzione è possibile controllare le applicazioni installate sui diversi computer e disinstallare le eventuali applicazioni non autorizzate presenti sui computer della rete.

Per disinstallare le applicazioni:

1. Selezionare la scheda **Ripara> Centro riparazioni** e fare clic su **Disinstallazione applicazioni**.



Screenshot 97: Disinstallazione applicazioni

2. Espandere l'applicazione per visualizzare l'elenco di computer, quindi selezionare i computer dove verrà disinstallata l'applicazione.

Nota

L'elenco di applicazioni visualizzate si basa sulle applicazioni non autorizzate configurate per il profilo di scansione in uso. For more information, refer to Configurazione della disinstallazione automatica delle applicazioni non autorizzate (page 126).

3. Ripetere il passaggio 2 per tutte le applicazioni da disinstallare, quindi fare clic su **Disinstalla**.

Nota

Immettere un criterio quindi fare clic su **Trova** per cercare la vulnerabilità. Per eliminare i risultati delle ricerche precedenti, fare clic su **Cancella**.

4. Configurare le opzioni descritte di seguito:

Table 61: Disinstallazione applicazioni

Opzione	Descrizione
Disinstalla immediatamente	Disinstalla immediatamente le applicazioni selezionate.
Disinstalla il	Disinstalla le applicazioni selezionate a una data e ora specifiche. Configurare quando disinstallare le applicazioni.
Credenziali	Selezionare il metodo di autenticazione da utilizzare o specificare un nome utente e una password. Selezionare **Utilizza credenziali computer se disponibili** per utilizzare le credenziali specificate nelle proprietà del computer. For more information, refer to Proprietà agente (page 49).
Opzioni preliminari alla distribuzione	Configurare le azioni da effettuare prima di distribuire le applicazioni selezionate. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).
Opzioni successive alla distribuzione	Configurare le azioni da effettuare dopo la distribuzione delle applicazioni selezionate. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).
Opzioni avanzate	Configurare altre opzioni relative al riavvio/arresto ed eliminare i file copiati dai computer remoti. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).

5. Fare clic su **OK**.

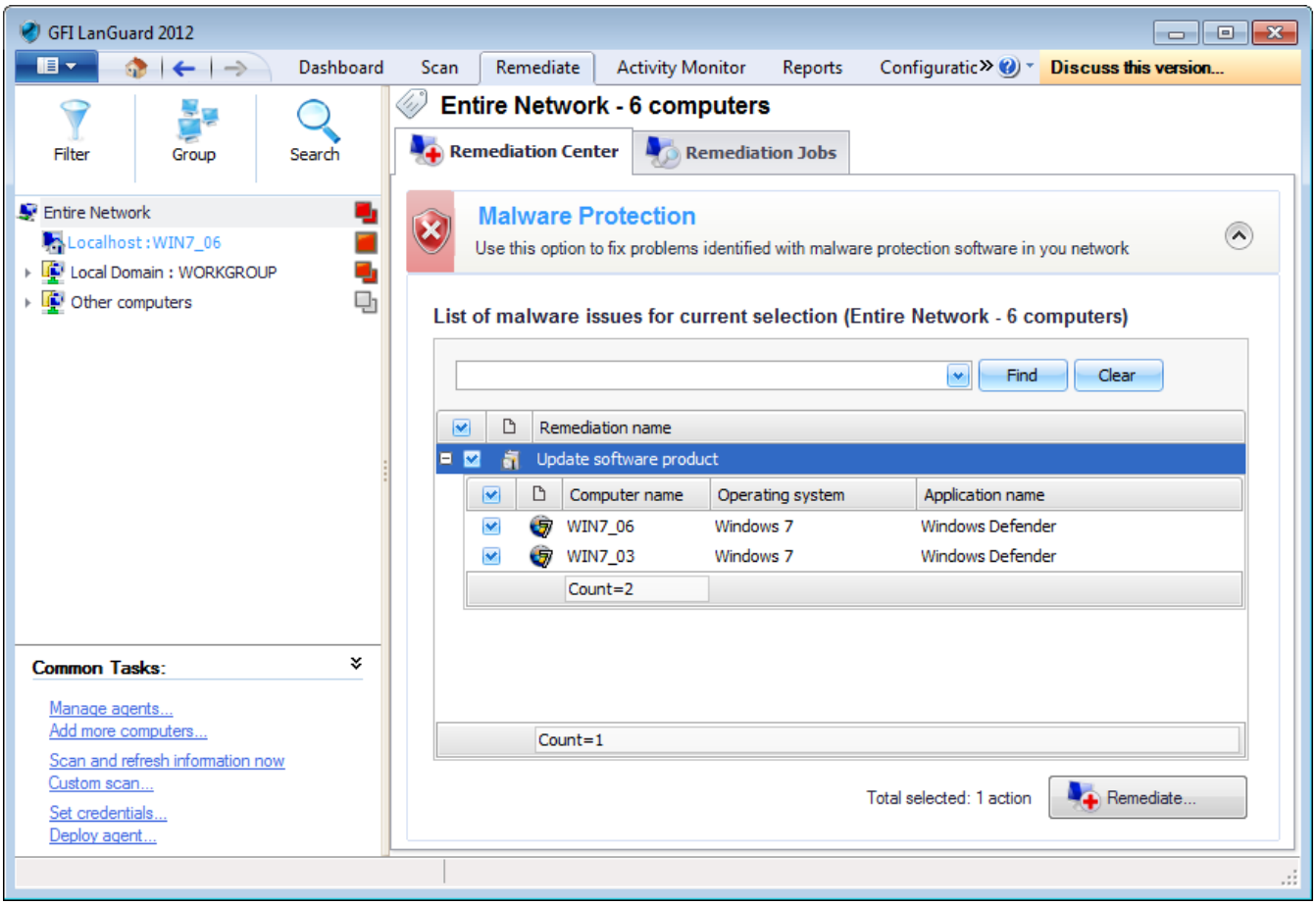
6. Per visualizzare l'avanzamento della disinstallazione, fare clic su **Operazioni di riparazione** dal pannello a destra.

8.2.7 Protezione antimalware

Utilizzare la sezione **Protezione antimalware** per risolvere le vulnerabilità legate alla protezione antimalware identificate nei computer di destinazione. Inoltre, questa sezione consente di scansionare i computer di destinazione alla ricerca di spyware, virus e abilitare il firewall locale.

Nota

Per scansionare un computer alla ricerca di virus e spyware, nel computer di destinazione deve essere installato un antivirus e un antispyware.



Screenshot 98: Protezione antimalware

Per rimediare le vulnerabilità di protezione antimalware:

1. Selezionare la scheda **Ripara> Centro riparazioni** e fare clic su **Protezione antimalware**.

2. Individuare ed espandere la vulnerabilità malware, quindi selezionare i computer da riparare.

> **Nota**
>
> Immettere un criterio quindi fare clic su **Trova** per cercare la vulnerabilità. Per eliminare i risultati delle ricerche precedenti, fare clic su **Cancella**.

3. Fare clic su Ripara e configurare le opzioni descritte di seguito:

Table 62: Opzioni di distribuzione

Opzione	Descrizione
Distribuisci immediatamente	Distribuisce immediatamente le applicazioni selezionate.
Distribuisci il	Distribuisce le applicazioni selezionate a una data e ora specifiche. Configurare quando distribuire le applicazioni.
Credenziali	Selezionare il metodo di autenticazione da utilizzare o specificare un nome utente e una password. Selezionare **Utilizza credenziali computer se disponibili** per utilizzare le credenziali specificate nelle proprietà del computer. For more information, refer to Proprietà agente (page 49).
Opzioni preliminari alla distribuzione	Configurare le azioni da effettuare prima di distribuire le applicazioni selezionate. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).

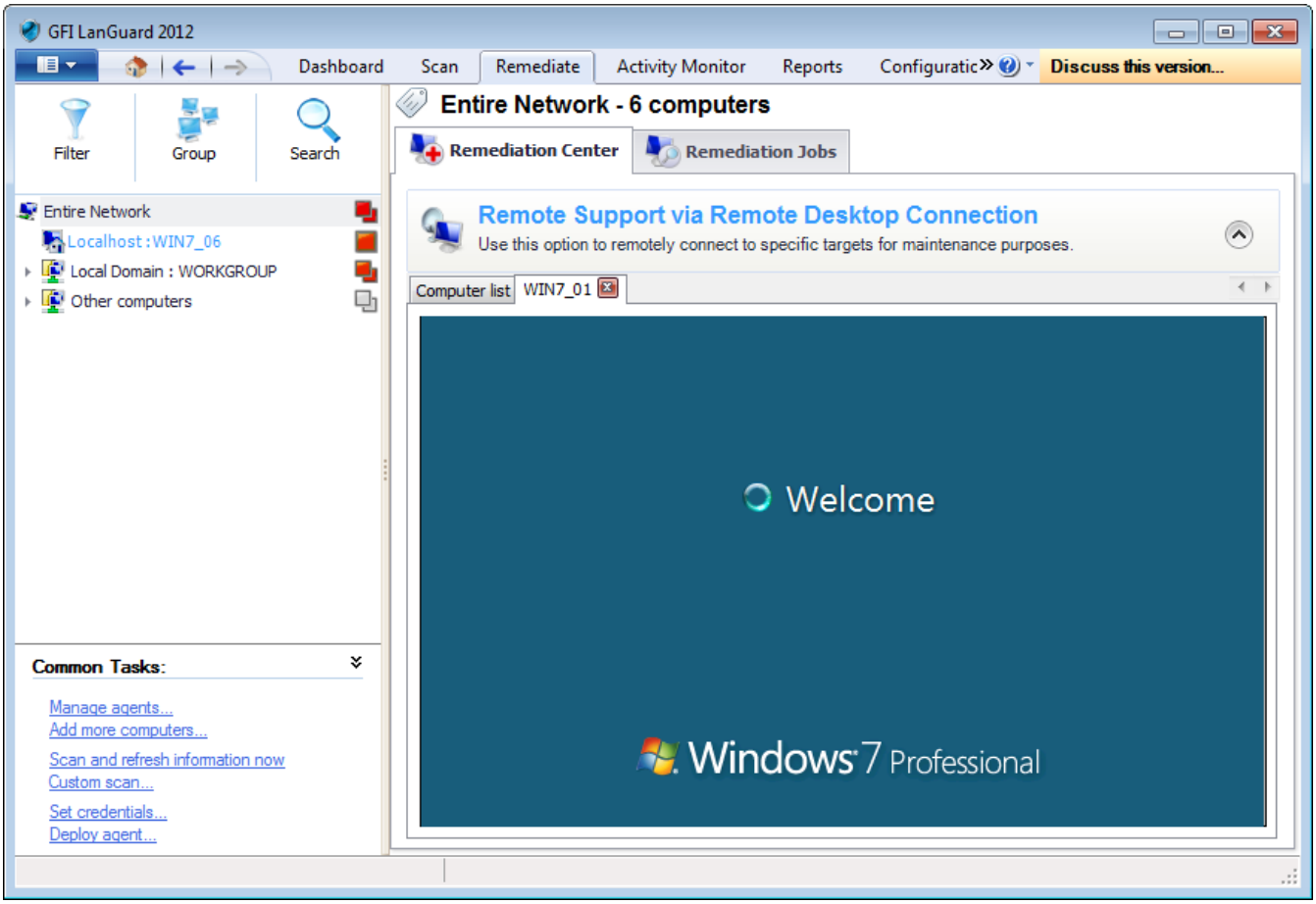
Opzione	Descrizione
Opzioni successive alla distribuzione	Configurare le azioni da effettuare dopo la distribuzione delle applicazioni selezionate. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).
Opzioni avanzate	Configurare altre opzioni relative al riavvio/arresto ed eliminare i file copiati dai computer remoti. For more information, refer to Configurazione delle opzioni di riparazione automatica (page 130).

4. Fare clic su **OK**.

5. Per visualizzare l'avanzamento dell'operazione, fare clic su **Operazioni di riparazione** nel pannello a destra.

8.2.8 Utilizzo del supporto del desktop remoto

Grazie al supporto remoto è possibile controllare computer remoti utilizzando i servizi terminale e il protocollo desktop remoto. Il supporto remoto consente di installare patch mancanti, service pack e software personalizzato tramite una connessione remota.



Screenshot 99: Connessione desktop remoto

Per connettersi in remoto a un computer di destinazione:

1. Fare clic sulla scheda **Ripara** e dal pannello a sinistra selezionare un computer o dominio/gruppo di lavoro.

2. Dal pannello a destra, espandere **Supporto remoto tramite connessione desktop remoto**.

3. A seconda della selezione effettuata, l'elenco contiene i computer disponibili che consentono la connessione desktop remoto.

4. Per eseguire la connessione, fare doppio clic su un computer dell'elenco.

Nota

Per disconnettere un computer, selezionare la scheda **Centro riparazioni>Supporto remoto tramite…**, fare clic con il pulsante destro del mouse su un computer dell'elenco e selezionare **Disconnetti**.

Nota

Per disabilitare la connessione remota, fare clic con il pulsante destro del mouse su un computer e selezionare **Disabilita connessione remota**.

9 Attività di monitoraggio

Il monitoraggio consente di ottenere maggiori informazioni sul modo in cui GFI LanGuard opera all'interno della propria infrastruttura. La scheda **Monitor attività** di GFI LanGuard consente di monitorare le scansioni di sicurezza attive, le operazioni di riparazione e i download degli aggiornamenti e delle definizioni di sicurezza mancanti.

Argomenti del presente capitolo:

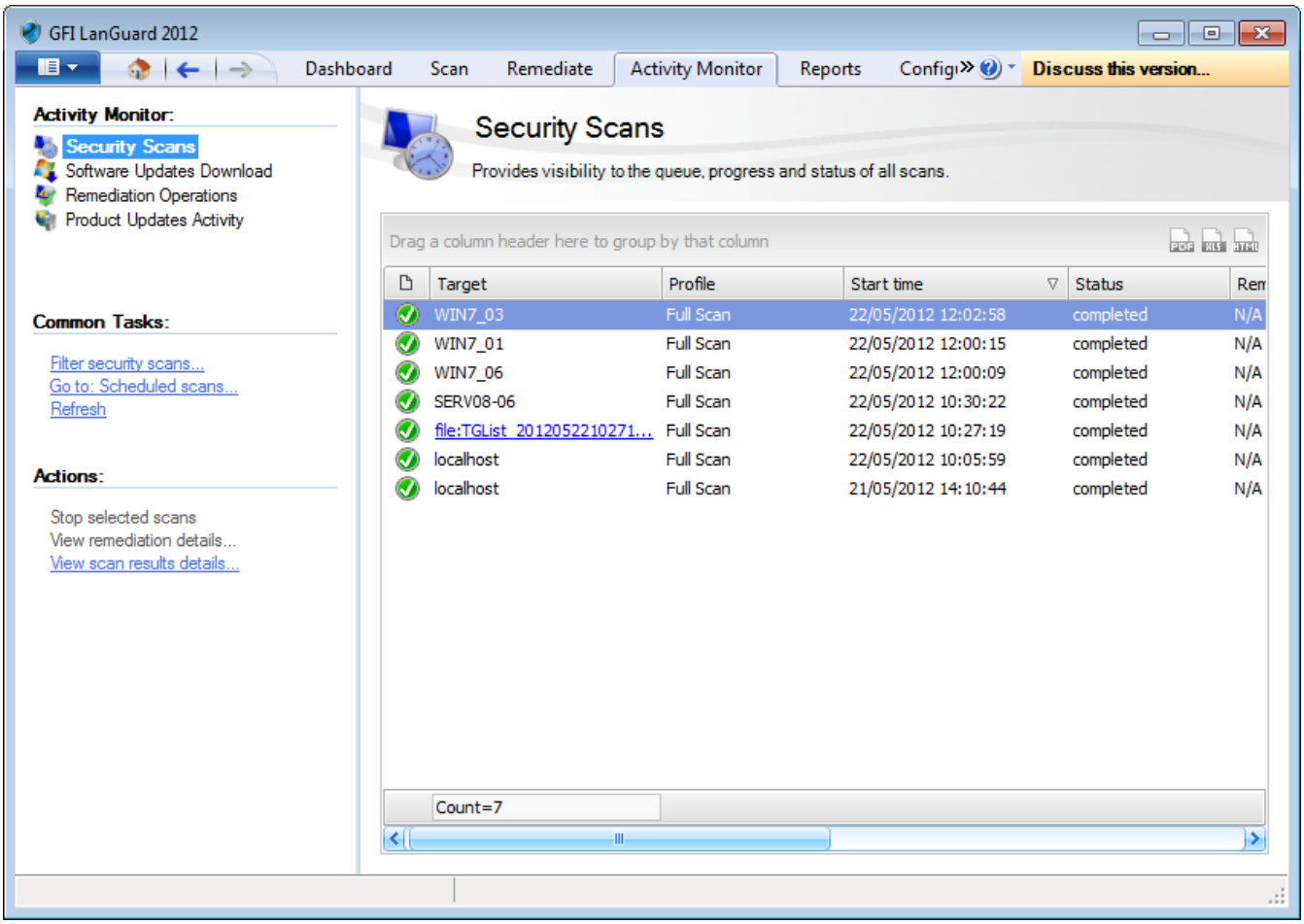
9.1 Monitoraggio scansioni di sicurezza 156
9.2 Monitoraggio download aggiornamenti software 158
9.3 Monitoraggio operazioni di riparazione 160
9.4 Monitoraggio aggiornamenti prodotto 163

9.1 Monitoraggio scansioni di sicurezza

La sezione **Scansioni di sicurezza** consente di monitorare tutte le scansioni di sicurezza attualmente in corso.

Per monitorare le scansioni di sicurezza attive:

1. Avviare GFI LanGuard.
2. Fare clic sulla scheda **Monitor attività** e dal riquadro di sinistra fare clic su **Scansioni di sicurezza**.



Screenshot 100: Monitoraggio scansioni di sicurezza

Nota

Per interrompere una scansione, fare clic con il pulsante destro del mouse sulla scansione e selezionare l'opzione **Interrompi scansioni selezionate**.

Nota

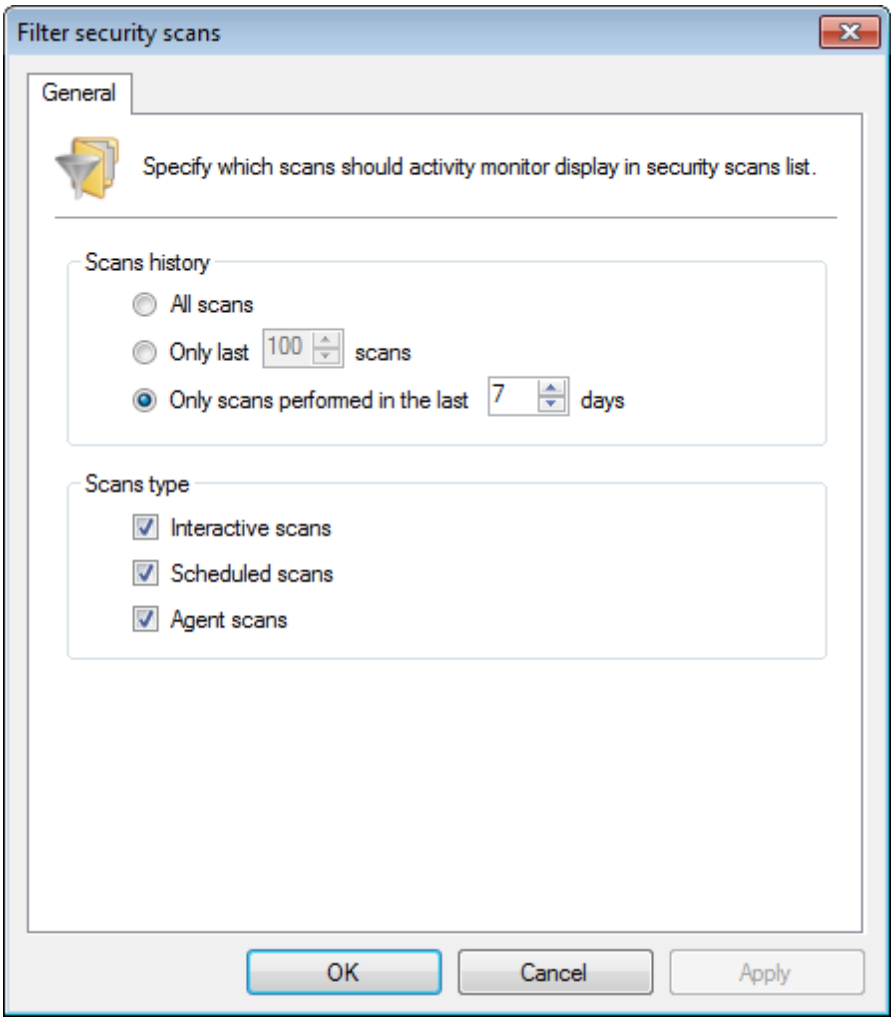
Per raggruppare i dati in base a criteri, trascinare l'intestazione di una colonna nell'area designata.

9.1.1 Filtra scansioni di sicurezza

La sezione **Scansione di sicurezza** consente di configurare il tipo di scansioni da monitorare. Per configurare il tipo di scansioni visualizzate:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Monitor attività** e da **Attività comuni** fare clic su **Filtra scansioni di sicurezza**.



Screenshot 101: Finestra di dialogo Filtra scansioni di sicurezza

3. Configurare le opzioni descritte di seguito:

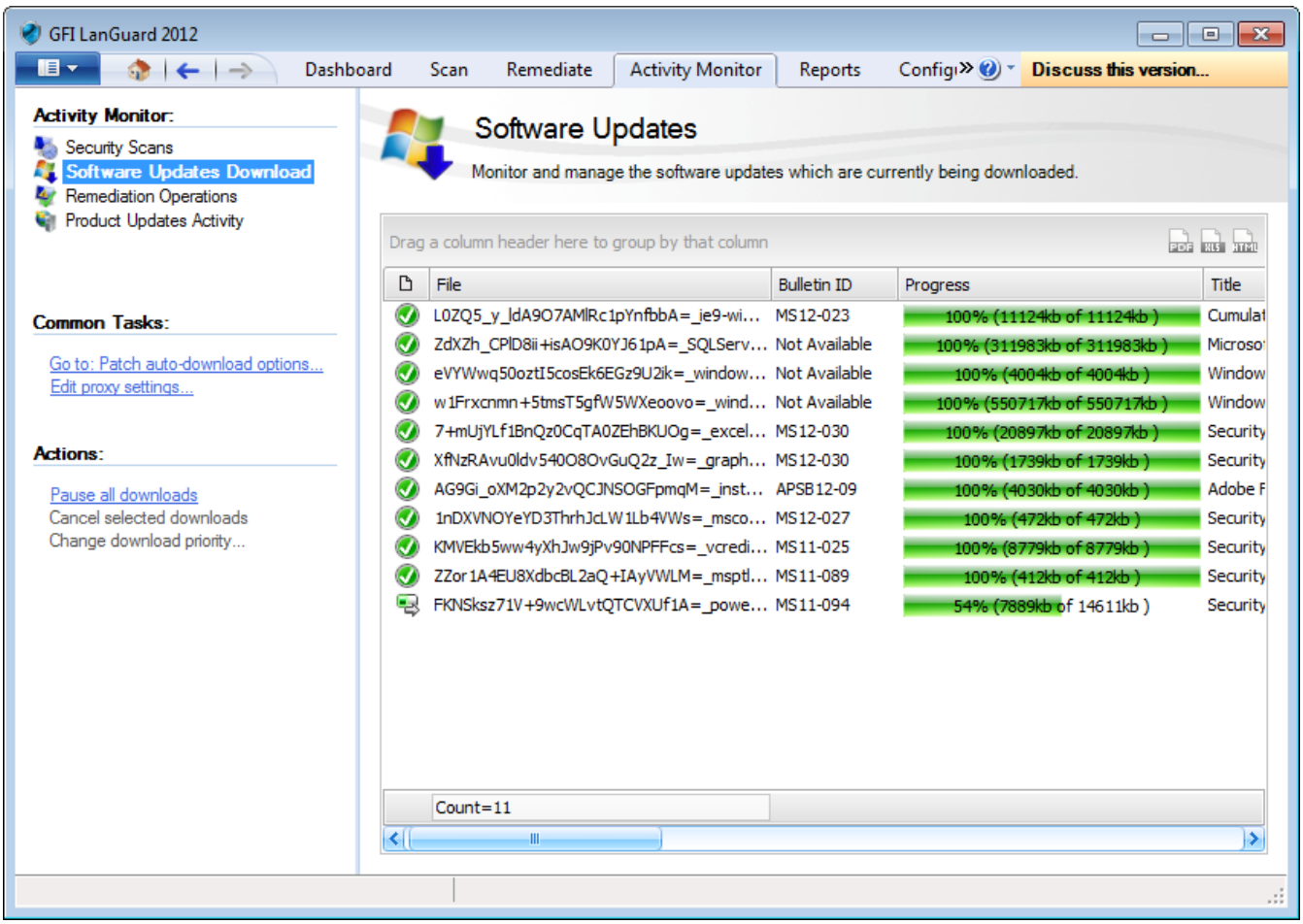
Table 63: Finestra di dialogo Filtra scansioni di sicurezza

Opzione	Descrizione
Tutte le scansioni	Visualizza tutte le scansioni.
Solo ultime x scansioni	Visualizza solo le ultime x scansioni.
Solo scansioni effettuate negli ultimi x giorni	Visualizza solo le scansioni effettuate negli ultimi x giorni.
Scansioni interattive	Visualizza solo le scansioni manuali. For more information, refer to Scansioni manuali (page 67).
Scansioni pianificate	Visualizza solo le scansioni pianificate. For more information, refer to Scansioni pianificate (page 72).
Scansioni agente	Visualizza solo le scansioni effettuate sui computer degli agenti. For more information, refer to Avvio di una scansione agente manuale (page 84).

4. Fare clic su **OK**.

9.2 Monitoraggio download aggiornamenti software

La schermata **Download aggiornamenti software** consente di monitorare, interrompere, annullare o modificare la priorità di tutti i download pianificati per le patch.


GFI LanGuard 2012
Dashboard
Scan
Remediate
Activity Monitor
Reports
Config
Discuss this version...
Activity Monitor:
Security Scans
Software Updates Download
Remediation Operations
Product Updates Activity
Common Tasks:
Go to: Patch auto-download options...
Edit proxy settings...
Actions:
Pause all downloads
Cancel selected downloads
Change download priority...
Software Updates
Monitor and manage the software updates which are currently being downloaded.
Drag a column header here to group by that column
File
Bulletin ID
Progress
Title
L0ZQ5_y_ldA9O7AMlRc1pYnfbbA=_je9-wi... MS12-023 100% (11124kb of 11124kb) Cumulat
ZdXZh_CPlD8ii+isAO9K0YJ61pA=_SQLServ... Not Available 100% (311983kb of 311983kb) Microso
eVYWwq50oztI5cosEk6EGz9U2ik=_window... Not Available 100% (4004kb of 4004kb) Window
w1Frxcnmn+5tmsT5gfW5WXeoovo=_wind... Not Available 100% (550717kb of 550717kb) Window
7+mUjYLf1BnQz0CqTA0ZEhBKUOg=_excel... MS12-030 100% (20897kb of 20897kb) Security
XfNzRAvu0ldv540O8OvGuQ2z_Iw=_graph... MS12-030 100% (1739kb of 1739kb) Security
AG9Gi_oXM2p2y2vQCJNSOGFpmqM=_inst... APSB12-09 100% (4030kb of 4030kb) Adobe F
1nDXVNOYeYD3ThrhJcLW1Lb4VWs=_msco... MS12-027 100% (472kb of 472kb) Security
KMVEkb5ww4yXhJw9jPv90NPFFcs=_vcredi... MS11-025 100% (8779kb of 8779kb) Security
ZZor1A4EU8XdbcBL2aQ+IAyVWLM=_msptl... MS11-089 100% (412kb of 412kb) Security
FKNSksz71V+9wcWLvtQTCVXUf1A=_powe... MS11-094 54% (7889kb of 14611kb) Security
Count=11

Screenshot 102: Download aggiornamenti di sicurezza

L'icona della prima colonna indica lo stato del download. La sottostante tabella illustra i vari stati:

Table 64: Stato download aggiornamenti

Icona	Descrizione
	Scaricato L'aggiornamento è stato scaricato.
	Download in corso L'aggiornamento è in fase di scaricamento.
	Non riuscito Si è verificato un errore durante il download dell'aggiornamento. Per ulteriori dettagli relativi all'errore riscontrato, fare riferimento alla colonna Errore.
	In sospeso L'aggiornamento è in coda per il download.
	Cancellato L'utente ha annullato il download dell'aggiornamento.

Fare clic con il pulsante destro del mouse su una voce e selezionare una delle opzioni descritte di seguito:

Table 65: Download aggiornamenti di sicurezza

Opzione	Descrizione
Configura download automatico patch	Abilita o disabilita il download automatico delle patch e viene utilizzato per la configurazione della posizione di archiviazione delle patch. Per ulteriori informazioni, consultare la sezione Impostazioni di download automatico patch.
Modifica impostazioni proxy...	Configura le impostazioni proxy utilizzate da GFI LanGuard per la connessione a Internet. For more information, refer to Configurazione aggiornamenti del programma (page 190).
Cambia priorità di download...	Modifica la priorità di download. Selezionare tra alta, normale o bassa.
Annulla download selezionati	Arresta e rimuove il download selezionato.
Sospendi tutti i download	Sospende temporaneamente tutti i download.

9.2.1 Risoluzione problemi aggiornamenti software non riusciti

La presente sezione offre le informazioni relative a tre errori di aggiornamento software, che probabilmente causeranno il mancato download e/o installazione degli aggiornamenti software.

La tabella sottostante riporta il messaggio effettivo che si riceve in presenza di uno degli errori, oltre alle possibili cause e soluzioni per ciascuno di essi:

Table 66: Risoluzione problemi aggiornamenti software non riusciti

Messaggio di errore	Causa	Soluzione
L'URL del file indica un file diverso da quello previsto. Tentare una nuova scansione con gli ultimi aggiornamenti del programma	Il fornitore di terze parti sostituisce le patch precedenti con quelle aggiornate, utilizzando il medesimo URL. GFI non controlla il modo in cui i fornitori di terze parti sostituiscono aggiornamenti e URL.	Scaricare manualmente gli aggiornamenti del prodotto più recenti ed eseguire una nuova scansione delle destinazioni. For more information, refer to Configurazione aggiornamenti del programma (page 190). **Nota** Vi è un ritardo dalle 12 alle 24 ore tra i rilasci di nuovi aggiornamenti da parte delle terze parti e il momento in cui GFI LanGuard fornisce il relativo supporto. Durante questo lasso di tempo, l'utente continuerà a ricevere il messaggio di errore, anche se scarica e scansiona le destinazioni mediante gli ultimi aggiornamenti del prodotto.
La cartella dell'archivio non è accessibile. Vedere Configurazione - Download automatico patch.	La cartella archivio è il percorso di download degli aggiornamenti. GFI LanGuard consente di specificare archivi alternativi oltre al percorso predefinito. Questo errore viene generalmente causato dopo aver specificato un percorso archivio non valido o inaccessibile (ad esempio, il percorso indicato fa riferimento a una posizione su un computer arrestato).	1. Controllare manualmente di poter accedere al percorso della cartella, utilizzando le medesime credenziali di accesso. 2. Assicurarsi che il percorso specificato sia valido: » **Percorso locale**, ad esempio: `C:\Share` o `C:\Folder` » **Percorso UNC**, ad esempio: `\\NetworkShare\Folder` 3. È necessario assicurarsi che il percorso sia digitato correttamente. **Nota** Per ulteriori informazioni, fare riferimento a **Configurazione impostazioni download automatico patch** alla sezione Configurazione distribuzione automatica aggiornamenti mancanti.
La connessione a Internet non è disponibile.	Il computer dove è installato GFI LanGuard non dispone di accesso a Internet. Esistono molte possibili cause a questo problema.	Stabilire una connessione a Internet e tentare il download degli aggiornamenti non riusciti.

9.3 Monitoraggio operazioni di riparazione

Le operazioni di riparazione possono essere monitorati dalle postazioni seguenti:

» dalla sottoscheda Operazioni di riparazione

» dalla visualizzazione Operazioni di riparazione

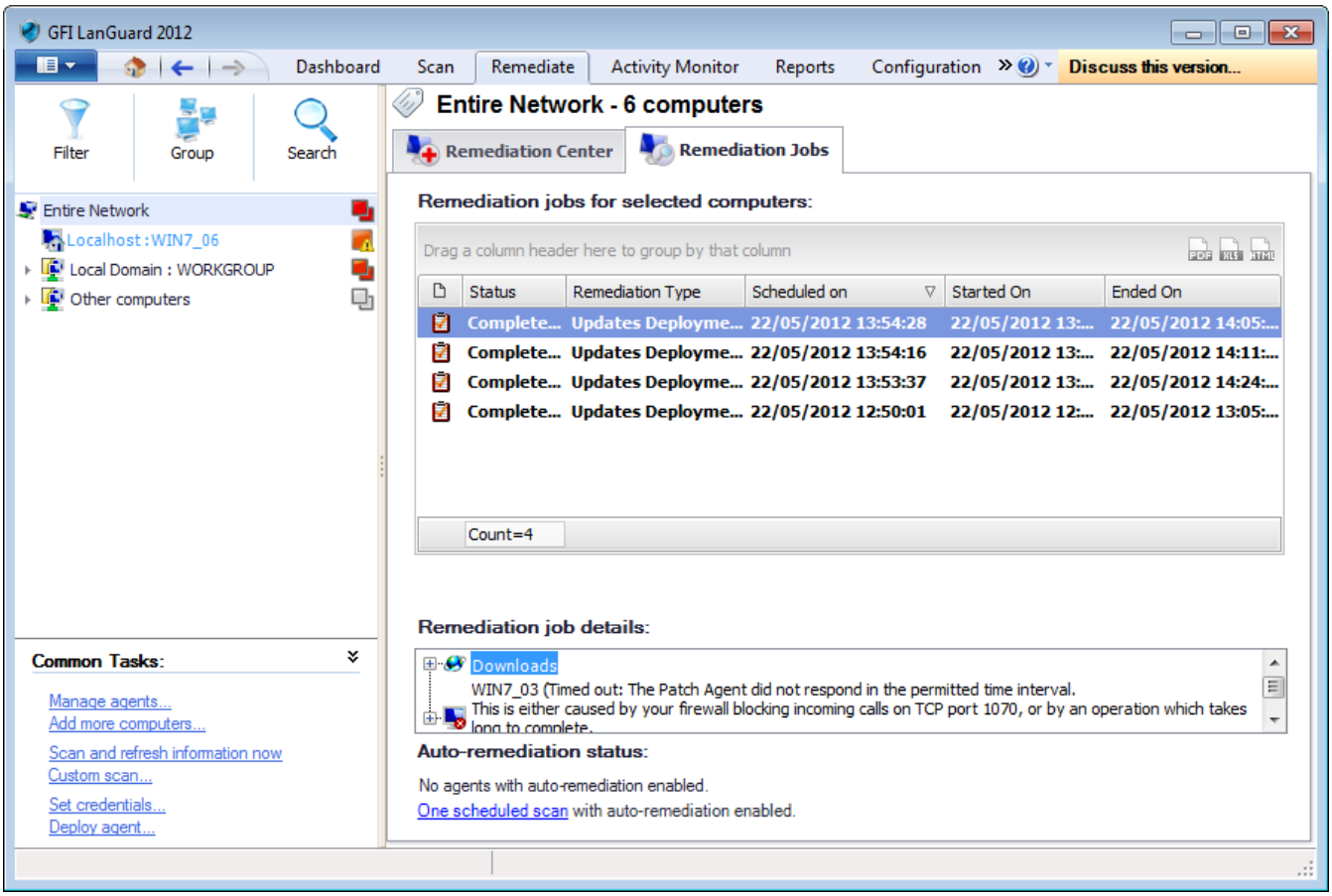
9.3.1 Sottoscheda Operazioni di riparazione

La sezione **Operazioni di riparazione** consente di monitorare le operazioni di riparazione in corso.

Per visualizzare le operazioni di riparazione in corso:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Ripara** sottoscheda **> Operazioni di riparazione**.



Screenshot 103: Monitoraggio delle operazioni dalla sottoscheda Operazioni di riparazione

3. Dalla struttura computer selezionare **Rete intera** per visualizzare tutte le operazioni in esecuzione e quelle completate. Selezionare computer/gruppi specifici per visualizzare la cronologia o l'avanzamento delle operazioni di riparazione per gli elementi selezionati.

Nota

Per interrompere l'operazione, fare clic con il pulsante destro del mouse su un'operazione di riparazione e selezionare **Annulla distribuzione selezionata**.

Nota

Fare clic con il pulsante destro del mouse su un'operazione di riparazione e selezionare **Vai alla scansione pianificata associata** per visualizzare la scansione preconfigurata che ha attivato la riparazione.

Nota

La sezione **Dettagli operazione di riparazione** fornisce i dettagli dell'avanzamento indicando il numero totale di file che devono essere scaricati, l'avanzamento del download per ciascun file e l'operazione corrente eseguita come parte dell'operazione di riparazione.

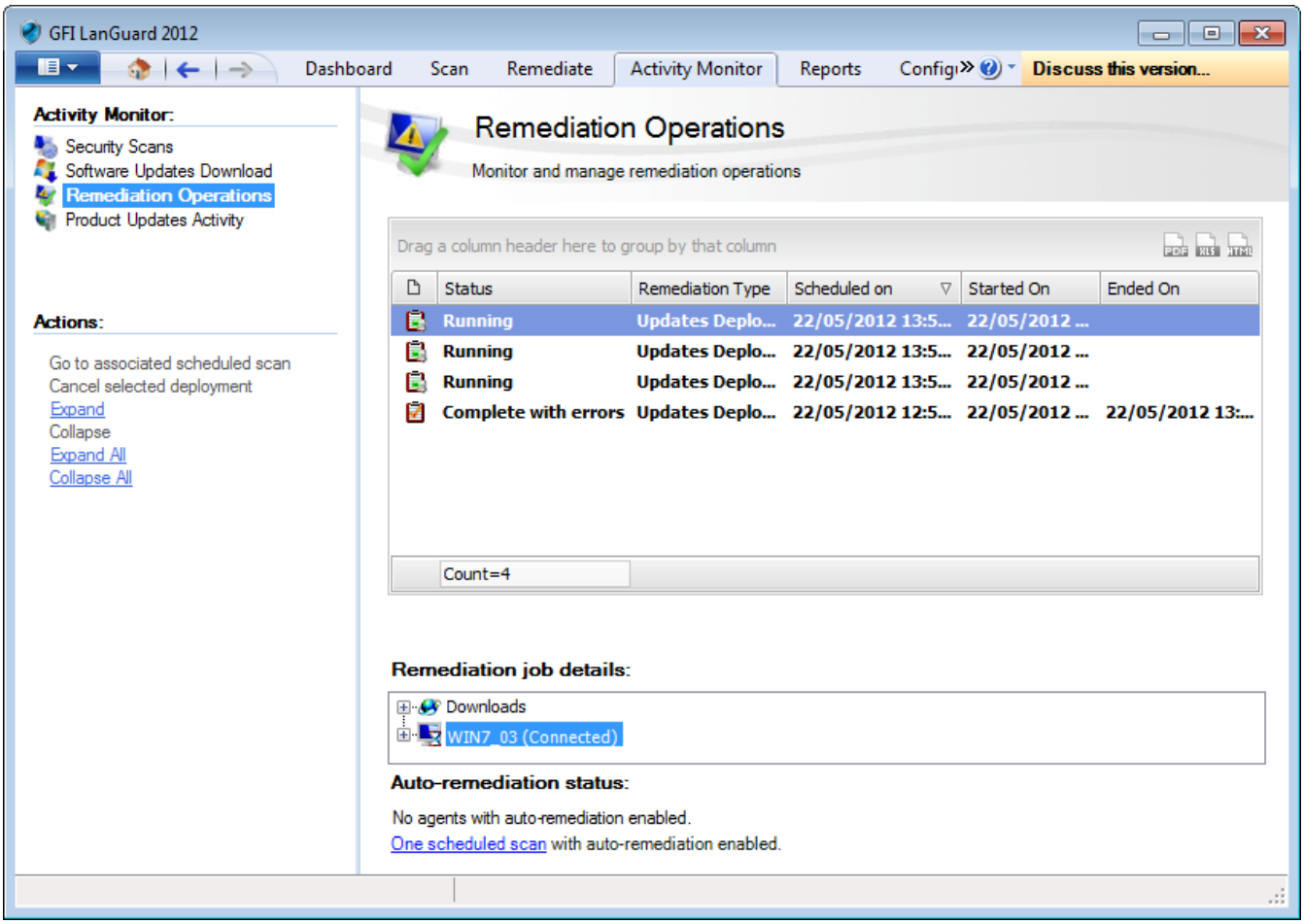
9.3.2 Visualizzazione Operazioni di riparazione

La schermata delle operazioni di riparazione consente di monitorare e annullare tutte le funzioni di riparazione pianificate all'interno di GFI LanGuard.

Per visualizzare l'attività delle operazioni di riparazione:

1. Avviare GFI LanGuard.

2. Fare clic su **Monitor attività > Operazioni di riparazione**.



Screenshot 104: Monitoraggio delle operazioni dalla visualizzazione Operazioni di riparazione

3. Utilizzare la visualizzazione per monitorare lo stato e la cronologia di tutte le operazioni di riparazione completate e in esecuzione.

> **Nota**
>
> Per interrompere l'operazione, fare clic con il pulsante destro del mouse su un'operazione di riparazione e selezionare **Annulla distribuzione selezionata**.

Nota

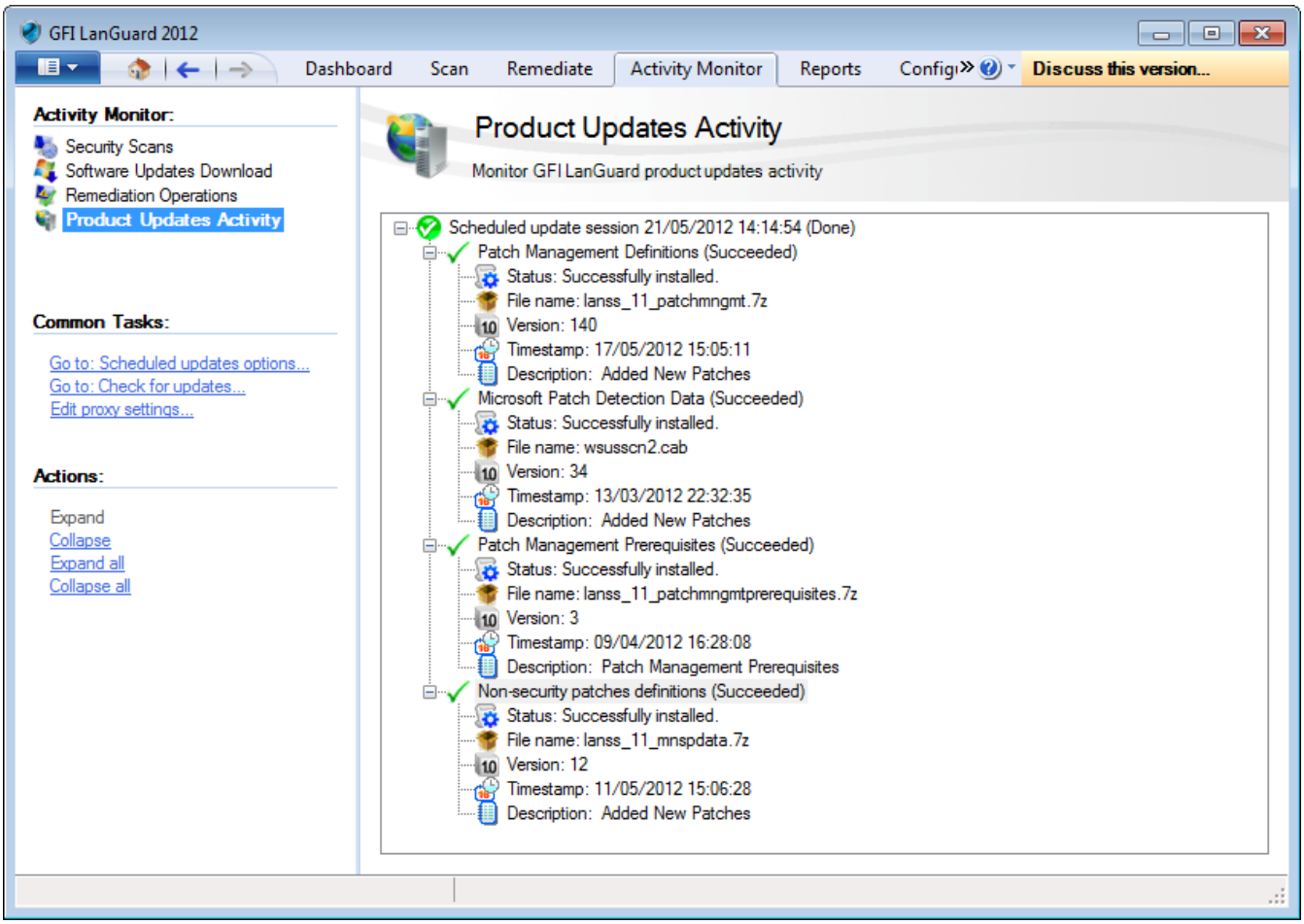
Fare clic con il pulsante destro del mouse su un'operazione di riparazione e selezionare **Vai alla scansione pianificata associata** per visualizzare la scansione preconfigurata che ha attivato la riparazione.

Nota

La sezione **Dettagli operazione di riparazione** fornisce i dettagli dell'avanzamento indicando il numero totale di file che devono essere scaricati, l'avanzamento del download per ciascun file e l'operazione corrente eseguita come parte dell'operazione di riparazione.

9.4 Monitoraggio aggiornamenti prodotto

La schermata **Attività aggiornamenti prodotto** consente di visualizzare una cronologia degli aggiornamenti del prodotto effettuati da GFI LanGuard. For more information, refer to Configurazione aggiornamenti del programma (page 190).



Screenshot 105: Attività aggiornamenti prodotto

10 Creazione di rapporti

GFI LanGuard include un modulo di creazione rapporti che consente di generare rapporti di testo e grafici sulla base delle informazioni ottenute dalle scansioni di sicurezza della rete. Il presente capitolo offre un anteprima dei rapporti disponibili oltre alle modalità per la creazione di rapporti personalizzati per una soluzione su misura. Dalla scheda Rapporti è possibile generare rapporti sull'attività tecnica per lo staff IT oltre a rapporti esecutivi che normalmente contengono meno dettagli tecnici e si concentrano maggiormente sulle statistiche generali.

Argomenti del presente capitolo:

10.1 Rapporti disponibili 164
10.2 Generazione report 171
10.3 Pianificazione dei rapporti 173
10.4 Personalizzazione rapporti predefiniti 176
10.5 Ricerca nel testo completo 180

10.1 Rapporti disponibili

La sezione seguente fornisce le informazioni relative ai rapporti disponibili per impostazione predefinita nella scheda **Rapporti** di GFI LanGuard. Sono disponibili due tipi di rapporti principali:

- **Rapporti generali**: comprendono rapporti tecnici dettagliati oltre a rapporti riepilogativi esecutivi relativi all'attività di protezione della LAN e di gestione delle patch
- **Rapporti di conformità legale**: forniscono informazioni sul sistema e sul controllo di rete che consentono di rispettare gli standard, le leggi e i regolamenti relativi all'utilizzo aziendale della rete e alle convenzioni di gestione.

Per ulteriori informazioni, fare riferimento alle seguenti sezioni:

- Rapporti generali disponibili
- Rapporti di conformità legale disponibili

10.1.1 Rapporti generali

Per visualizzare i rapporti **Generali**:

1. Fare clic sulla scheda **Rapporti**.
2. Dall'elenco dei rapporti, espandere la sezione **Generali** quindi scegliere uno dei seguenti:

Table 67: Rapporti generali disponibili

Titolo del rapporto	Descrizione
Panoramica sicurezza di rete	Un rapporto di riepilogo esecutivo che visualizza: » Livello di vulnerabilità di rete » Computer più vulnerabili » Stato agente » Stato controllo » Tendenze della vulnerabilità nel tempo » Informazioni sui sistemi operativi » Server e workstation
Panoramica sicurezza computer	Un rapporto di riepilogo esecutivo che visualizza: » Livello di vulnerabilità computer » Stato agente » Stato controllo » Tendenze della vulnerabilità nel tempo » Riepilogo computer e dettagli
Stato vulnerabilità	Illustra informazioni statistiche relative alle vulnerabilità rilevate sui computer di destinazione. Le vulnerabilità possono essere raggruppate per: » Nome computer » Gravità vulnerabilità » Timestamp » Categoria
Stato dell'applicazione di patch	Mostra le informazioni statistiche relative agli aggiornamenti mancanti e installati rilevati sulle destinazioni di scansione. Gli aggiornamenti possono essere raggruppati per nome, gravità, timestamp, fornitore e categoria. Utilizzare questo rapporto per ottenere: » Confronto tra aggiornamenti mancanti e aggiornamenti installati » I grafici e le tabelle che riportano la distribuzione degli aggiornamenti mancanti per ciascun elemento dei primi e secondi criteri di raggruppamento » I grafici e le tabelle che riportano la distribuzione degli aggiornamenti installati per ciascun elemento dei primi e secondi criteri di raggruppamento » Dettagli applicazione patch per le patch mancanti e installate.
Aggiornamenti di sicurezza Microsoft® mancanti	Mostra le informazioni statistiche relative agli aggiornamenti di sicurezza Microsoft® mancanti rilevati sulle destinazioni di scansione. Selezionare gli elementi da includere nel rapporto: » Tabellone di distribuzione generale degli aggiornamenti mancanti » Tabella di distribuzione » Elenco vulnerabilità.
Aggiornamenti di sicurezza non Microsoft® mancanti	Mostra le informazioni statistiche relative agli aggiornamenti di sicurezza non Microsoft® mancanti rilevati sulle destinazioni di scansione. Selezionare gli elementi da includere nel rapporto: » Tabellone di distribuzione generale degli aggiornamenti mancanti » Tabella di distribuzione » Elenco vulnerabilità.
Aggiornamenti di sicurezza mancanti	Illustra informazioni statistiche relative agli aggiornamenti di sicurezza mancanti rilevati sui computer sottoposti a scansione.

Titolo del rapporto	Descrizione
Controllo completo	Un rapporto tecnico che illustra le informazioni rilevate durante un controllo. Inoltre, il rapporto contiene informazioni su: » Vulnerabilità » Porte aperte » Hardware e software
Riepilogo computer	Un riepilogo delle informazioni della destinazione di scansione, tra cui: » Informazioni sul sistema operativo » Stato agente » Gravità vulnerabilità
Verifica hardware	Fornisce informazioni relative all'hardware rilevato durante un controllo.
Dettagli computer	Fornisce un elenco dettagliato delle proprietà del computer, incluse: » Indirizzo MAC » Durata (TTL) » Ruolo di rete » Dominio » LAN Manager » È agente relay » Utilizza un agente relay » Attributi » Sistema operativo » Indirizzo IP.
Condivisioni aperte	Elenca tutte le cartelle condivise rilevate durante un controllo. I risultati sono raggruppati in base al nome del computer.
Porte aperte	Elenca tutte le porte aperte rilevate durante un controllo. Il risultato è raggruppato in base al tipo di porta (TCP e UDP).
Basato su scansione - Controllo completo	Un rapporto tecnico che illustra le informazioni rilevate durante la scansione specificata. Il rapporto contiene i dettagli completi dei computer sottoposti a scansione, oltre alle operazioni di riparazione automatica effettuate dopo la scansione.
Riepilogo ultima scansione	Un rapporto tecnico contenente un riepilogo di tutte le informazioni rilevate durante l'ultima scansione.
Dettagli ultima scansione	Un rapporto tecnico contenente tutte le informazioni rilevate durante l'ultima scansione, contenente i dettagli completi della destinazione di scansione.
Ultima riparazione automatica	Un rapporto tecnico contenente tutte le informazioni relative alle riparazioni automatiche effettuate dopo l'ultima scansione.
Modifiche di sicurezza ultima scansione	Visualizza tutte le modifiche rilevate durante l'ultima scansione.
Controllo software	Visualizza tutte le applicazioni non autorizzate installate nei computer di destinazione rilevate durante un controllo. Inoltre, il rapporto comprende informazioni su: » Antivirus » Antispyware » Inventario applicazioni
Applicazioni non autorizzate	Elenca tutte le applicazioni non autorizzate installate nelle destinazioni di scansione.

Titolo del rapporto	Descrizione
Applicazioni antivirus	Visualizza informazioni relative all'antivirus installato nelle destinazioni di scansione.
Cronologia di scansione	Una panoramica dei controlli di sicurezza di rete eseguiti nel tempo. Inoltre, il rapporto comprende informazioni su: » Computer più scansionati » Computer meno scansionati » Stato di controllo » Elenco cronologia
Cronologia riparazioni	Visualizza informazioni relative alle operazioni di riparazione eseguite nei computer di destinazione. Inoltre, il rapporto comprende informazioni su: » Azioni di riparazione per giorno » Distribuzione riparazione per categoria » Elenco di riparazioni raggruppato per computer
Cronologia sicurezza di rete	Visualizza le modifiche effettuate nelle destinazioni di scansione tra i controlli. Inoltre, il rapporto comprende le modifiche relative a: » Livello di vulnerabilità » Account utente » Gruppi » Porte » Condivisioni » Voci del registro di sistema
Confronto di base	Consente di confrontare i risultati di tutte le destinazioni di scansione rispetto a un computer di base. Dall'elenco a discesa, selezionare i computer di base e fare clic su Genera. I risultati sono raggruppati in base al nome del computer e includono, tra l'altro, informazioni su: » Registro di sistema » Service pack e aggiornamenti cumulativi installati » Aggiornamenti di sicurezza/non di sicurezza mancanti » Livello di vulnerabilità

10.1.2 Rapporti di conformità legale

Per visualizzare i rapporti di **Conformità legale**:

1. Fare clic sulla scheda **Rapporti**.

2. Dall'elenco dei rapporti espandere una delle seguenti suite di rapporti di conformità, quindi scegliere quello da generare:

Table 68: Rapporti di conformità legale disponibili

Titolo report suite	Descrizione
Rapporti di conformità PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) è uno standard di sicurezza delle informazioni per organizzazioni che trattano informazioni del titolare della carta delle principali carte di debito, credito, prepagate, e-purse, ATM, e POS. GFI LanGuard offre una serie di rapporti che rispondono ai requisiti di conformità PCI DSS, tra cui: » Requisito 1.4 PCI DSS - Applicazioni firewall installate » Requisito 2.2.3 PCI DSS - Applicazioni di crittografia unità » Requisito 5.2 PCI DSS - Applicazioni antivirus » Requisito 6.1 PCI DSS - Cronologia riparazioni per data » Requisito 12.12 PCI DSS - Porte trojan aperte per host.
Rapporti di conformità HIPAA	Health Insurance Portability and Accountability Act (HIPAA) è un requisito di tutti i fornitori di servizi sanitari che regola lo scambio dei dati privati dei pazienti. Ciò consente di evitare la divulgazione o la pubblicazione illegale di informazioni di natura medica. Per facilitare il rispetto dei regolamenti HIPAA, GFI LanGuard offre una suite di rapporti di conformità HIPAA, tra cui: » HIPAA 164.308(a)(1)(ii)(A) - Aggiornamenti di sicurezza mancanti per host » HIPAA 164.308(a)(1)(ii)(A) - Distribuzione vulnerabilità per host » HIPAA 164.308(a)(4)(ii)(A) - Porte aperte » HIPAA 164.308(a)(5)(ii)(D) - Criterio di controllo » HIPAA 164.308(a)(8) - Confronto modifiche di base.
Rapporti di conformità SOX	Sarbanes-Oxley Act (SOX) è una regolamentazione creata in risposta agli scandali finanziari ad alto profilo oltre che per proteggere gli azionisti e il pubblico generale dagli errori di contabilità e dalle pratiche fraudolente all'interno dell'azienda. GFI LanGuard offre un elenco di rapporti di conformità SOX, tra cui: » SOX 302.a - Riepilogo vulnerabilità della rete » SOX 302.a - Cronologia riparazioni per host » SOX 302.a - Cronologia scansioni di sicurezza » SOX 404 - Elenco vulnerabilità per categoria » SOX 404 - Aggiornamenti di sicurezza mancanti per host.
Rapporti di conformità GLBA	Il Gramm-Leach-Bliley Act (GLBA) è una legge che consente la consolidazione tra banche e compagnie di assicurazione. Una parte della legge si focalizza sulla conformità della rete IT per dette aziende. GFI LanGuard offre un elenco di rapporti di conformità GLBA, tra cui: » GLBA 501.b - Confronto modifiche di base » GLBA 501.b - Stato dell'applicazione di patch alla rete » GLBA 501.b - Porte trojan aperte per host » GLBA 501.b - Host vulnerabili sulla base delle porte aperte » GLBA 501.b - Host vulnerabili per livello di vulnerabilità.
Rapporti di conformità PSN CoCo	Il Public Service Network - Code of Connection (PSN CoCo) è semplicemente un elenco di condizioni che dovrebbero essere rispettate prima di connettere una rete accreditata a un'altra. GFI LanGuard consente di monitorare lo stato di tali connessioni attraverso un elenco di rapporti di conformità PSN CoCo, che comprendono: » PSNCoCo RIS. 1 - Confronto modifiche di base » PSNCoCo MAL. 1- Applicazioni di crittografia unità » PSNCoCo MAL. 1 - Applicazioni firewall installate » PSNCoCo PAT. 1 - Aggiornamenti di sicurezza installati per host » PSNCoCo PAT. 1 - Aggiornamenti di sicurezza installati per gravità.

Titolo report suite	Descrizione
Rapporti di conformità FERPA	Il Family Educational Rights and Privacy Act (FERPA) è una legge federale che tutela la privacy dei record dell'istruzione degli studenti. La legge si applica a tutte le scuole che ricevono fondi in base a un programma attuato dall'U.S. Department of Education. GFI LanGuard offre un elenco di rapporti di conformità FERPA, tra cui: » FERPA 20 USC 1232g (b) - Stato dell'applicazione di patch alla rete » FERPA 20 USC 1232g (b) - Registro di sicurezza della rete per host » FERPA 20 USC 1232g (b) - Cronologia riparazioni per data » FERPA 20 USC 1232g (b) - Distribuzione vulnerabilità per host » FERPA 20 USC 1232g (b) - Host vulnerabili sulla base delle porte aperte.
Rapporti di conformità ISO/IEC 27001 e 27002	Lo standard Information technology – Security techniques – Information security management systems (ISO/IEC) formalmente indica un sistema di gestione inteso a portare la sicurezza delle informazioni sotto il controllo esplicito della gestione. GFI LanGuard offre un vasto elenco di rapporti di conformità ISO/IEC, tra cui: » ISO/IEC 27001 A. 10.4 - Applicazioni antivirus » ISO/IEC 27001 A. 10.7.2 - Applicazioni di crittografia unità » ISO/IEC 27001 A. 10.6.2 - Condivisioni aperte » ISO/IEC 27001 A. 10.6.2 - Servizi » ISO/IEC 27001 A. 10.6.2 - Informazioni di sistema.
Rapporti di conformità FISMA	Il Federal Information Security Management Act (FISMA) assegna responsabilità specifiche alle agenzie federale, al National Institute of Standards and Technology (NIST) e all'Office of Management and Budget (OMB) al fine di rafforzare la sicurezza del sistema di informazioni. Nello specifico, FISMA richiede che il capo di ciascuna agenzia implementi politiche e procedure volte a una riduzione a un livello accettabile dei costi legati ai rischi per la sicurezza delle informazioni. GFI LanGuard consente di essere conformi agli standard FISMA attraverso i rapporti forniti, che includono: » FISMA NIST SP 800-53 AC-2 - Gruppi e utenti » FISMA NIST SP 800-53 PM-5 - Dettagli computer » FISMA NIST SP 800-53 PM-5 - Riepilogo computer » FISMA NIST SP 800-53 SI-5 - Aggiornamenti di sicurezza mancanti per host » FISMA NIST SP 800-53 SI-7 - Applicazioni antivirus.
Rapporti di conformità CAG	Il Consensus Audit Guidelines (CAG) è una pubblicazione di linee guida delle best practice per la sicurezza dei computer. Il progetto è stato avviato in risposta ad estreme perdite di dati subite dalle organizzazioni di una base industriale della difesa statunitense. GFI LanGuard offre un elenco di rapporti di conformità CAG, tra cui: » CAG CC1 - Verifica hardware » CAG CC1 - Cronologia di scansione » CAG CC3 - Criterio di controllo » CAG CC3 - Vulnerabilità di sicurezza di livello basso » CAG CC11 - Porte aperte.

Titolo report suite	Descrizione
Rapporti di conformità NERC CIP	Il North American Electric Reliability Corporation (NERC) sviluppa gli standard per il funzionamento di sistemi di trasmissione di energia elettrica, monitorando e attuando il rispetto di tali standard, valutando l'adeguatezza delle risorse e fornendo risorse educative e formative come parte di un programma di accreditamento, al fine di assicurare che gli operatori dei sistemi di trasmissione di energia elettrica rimangano qualificati e competenti. GFI LanGuard offre un elenco di rapporti di conformità NERC CIP, tra cui: » NERC CIP-005 R2 - Applicazioni firewall installate » NERC CIP-005 R2 - Porte aperte » NERC CIP-007 R2 - Condivisioni aperte » NERC CIP-007 R2 - Servizi » NERC CIP-007 R2 - Informazioni di sistema.

10.2 Generazione report

GFI LanGuard viene fornito con un elenco esteso di rapporti predefiniti. Possono essere utilizzati come sono, oppure modificati per fornire informazioni specifiche per i propri requisiti.

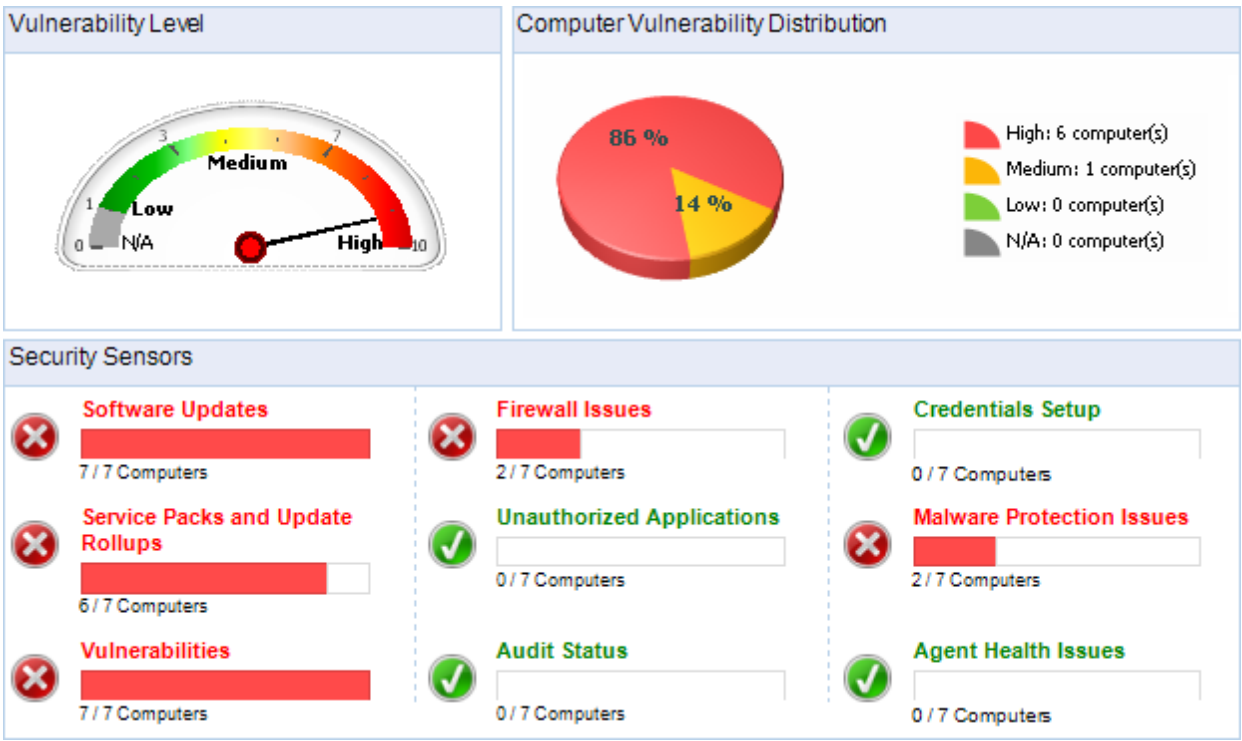
> **Nota**
>
> For more information, refer to Personalizzazione rapporti predefiniti (page 176).

Per generare un rapporto:

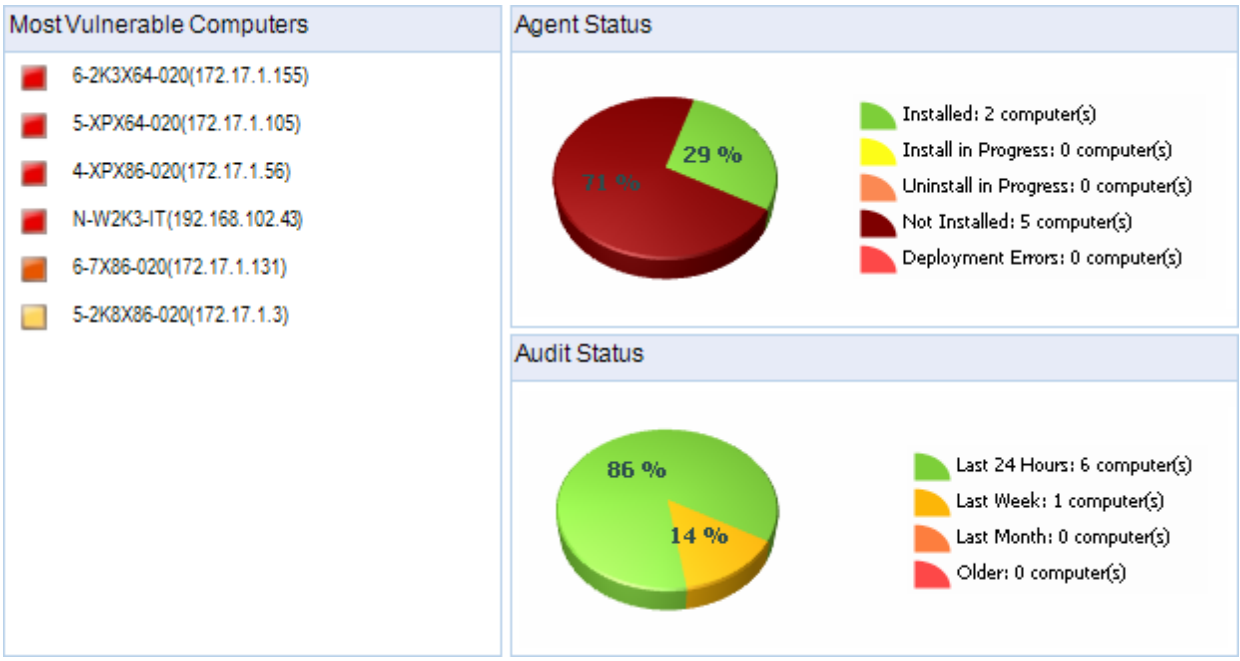
1. Fare clic sulla scheda **Rapporti**.
2. Dalla struttura computer selezionare il computer/gruppo per il rapporto.

> **Nota**
>
> Selezionare **Rete intera** per il rapporto su tutti i computer elencati nella struttura computer.

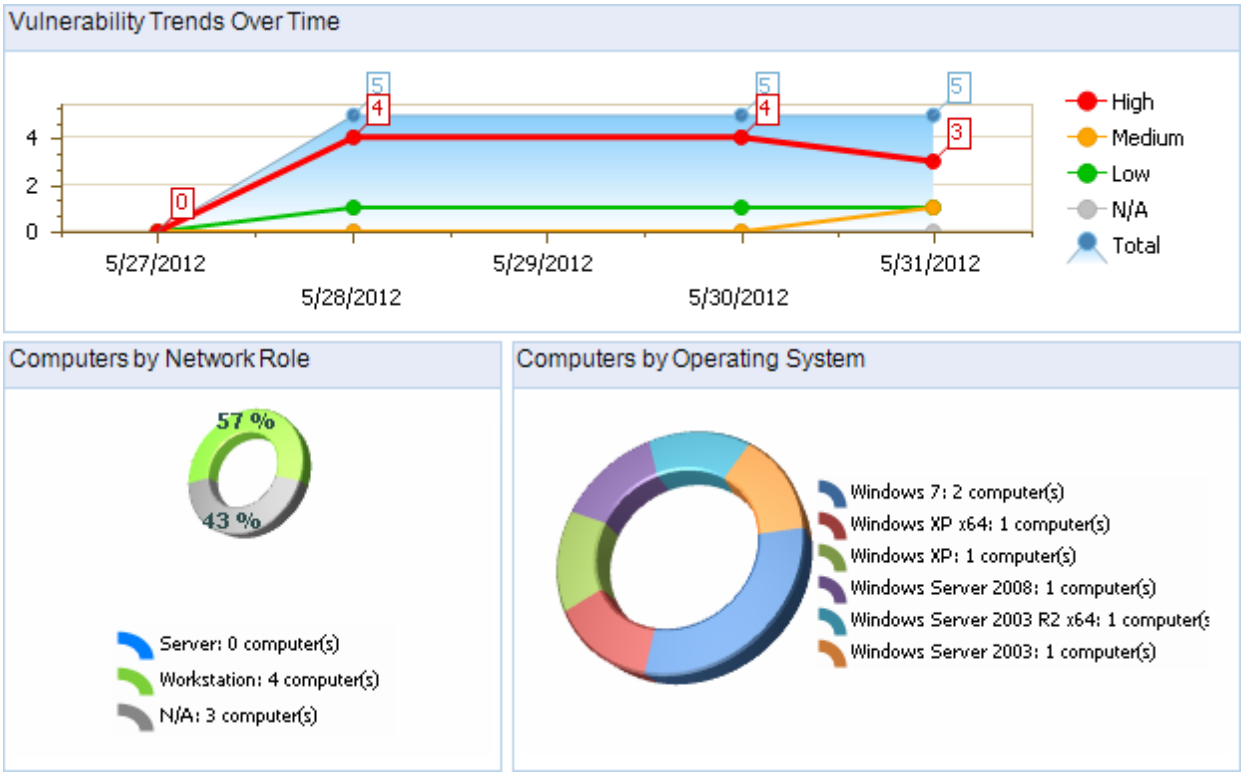
3. Dall'elenco dei rapporti selezionare il rapporto da generare.
4. (Facoltativo) Dal riquadro a destra, selezionare **Personalizza rapporto** per effettuare modifiche agli elementi del rapporto.
5. Fare clic su **Genera rapporto**.



Screenshot 106: Rapporto di esempio - Parte 1



Screenshot 107: Rapporto di esempio - Parte 2



Screenshot 108: Rapporto di esempio - Parte 3

10.3 Pianificazione dei rapporti

Per automatizzare le attività di creazione di rapporti, GFI LanGuard consente di generare ed eventualmente inviare i rapporti, in base a una pianificazione. È possibile configurare le pianificazioni per i rapporti esistenti o per quelli personalizzati.

Questa sezione contiene informazioni relative a:

- Creazione di nuovi rapporti pianificati
- Configurazione opzioni rapporti pianificati
- Gestione rapporti pianificati

10.3.1 Creazione di nuovi rapporti pianificati

Per creare un nuovo rapporto pianificato:

1. Fare clic sulla scheda **Rapporti**.

2. Da **Azioni**, selezionare **Nuovo rapporto pianificato**.

1
Report Template
Schedule Report Template:
Network Security Overview
Schedule Report Name:
Schedule for report 'Network Security Overview'
Schedule Report Description:
An executive summary report showing network vulnerability level, most vulnerable computers, agent status and audit status, vulnerability trends over time, information on operating systems, servers and

Screenshot 109: Selezionare il modello del rapporto pianificato

3. Dalla sezione **Modello rapporto**, configurare le seguenti opzioni:

Table 69: Opzioni modello del rapporto pianificato

Opzione	Descrizione
Modello rapporto pianificato	Selezionare un rapporto esistente dall'elenco a discesa. Consente di creare un nuovo rapporto sulla base delle impostazioni di un rapporto esistente.
Nome rapporto pianificato	Digitare un nome univoco per il nuovo rapporto.
Descrizione rapporto pianificato	In alternativa, digitare alcune informazioni relative al rapporto, come gli elementi dello stesso o le impostazioni di pianificazione.

Screenshot 110: Aggiunta o rimozione di domini di destinazione e/o computer

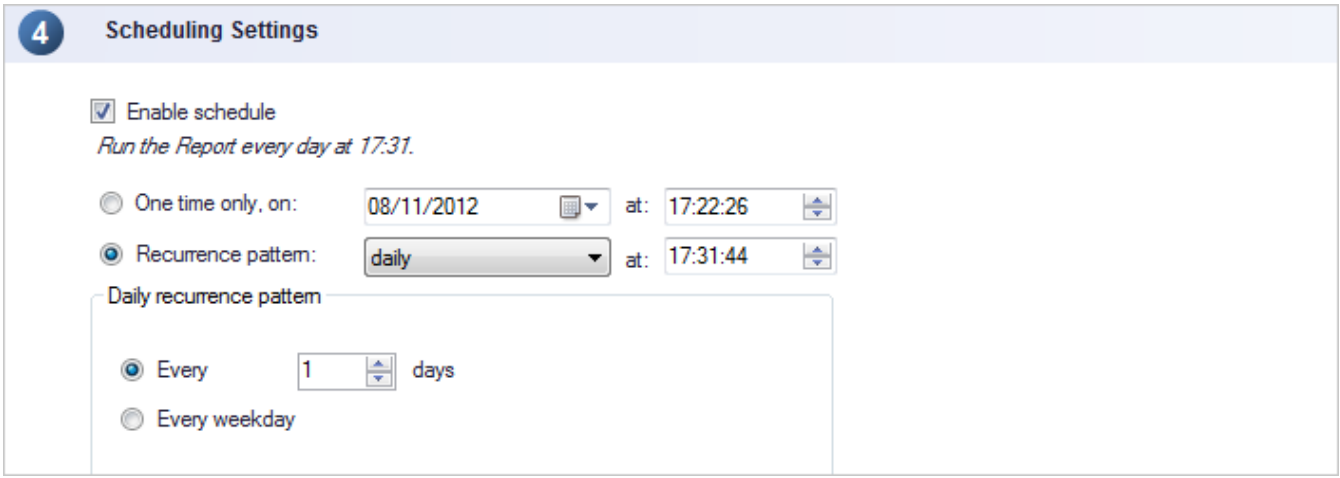
4. Dalla sezione **Domini e computer di destinazione**, configurare le seguenti opzioni:

Table 70: Opzioni Domini e computer di destinazione

Opzione	Descrizione
	Dalla struttura computer, selezionare il dominio o il gruppo di lavoro e fare clic su **Aggiungi dominio**. I domini/gruppi di lavoro selezionati vengono aggiunti al rapporto.
	Fare clic su **Aggiungi IP** per aprire la finestra di dialogo **Aggiungi intervallo indirizzi IP**. Dalla finestra di dialogo **Aggiungi intervallo indirizzi IP**, definire un intervallo indirizzi IP o subnet e fare clic su **OK**.
	Selezionare il dominio/gruppo di lavoro/intervallo IP da rimuovere e fare clic su **Rimuovi dominio/IP**.

5. Dall'elenco a discesa **Filtro**, selezionare un filtro da applicare al nuovo rapporto pianificato. In tal modo è possibile generare rapporti sulla base dei dati relativi alle destinazioni di scansione incluse nel filtro.

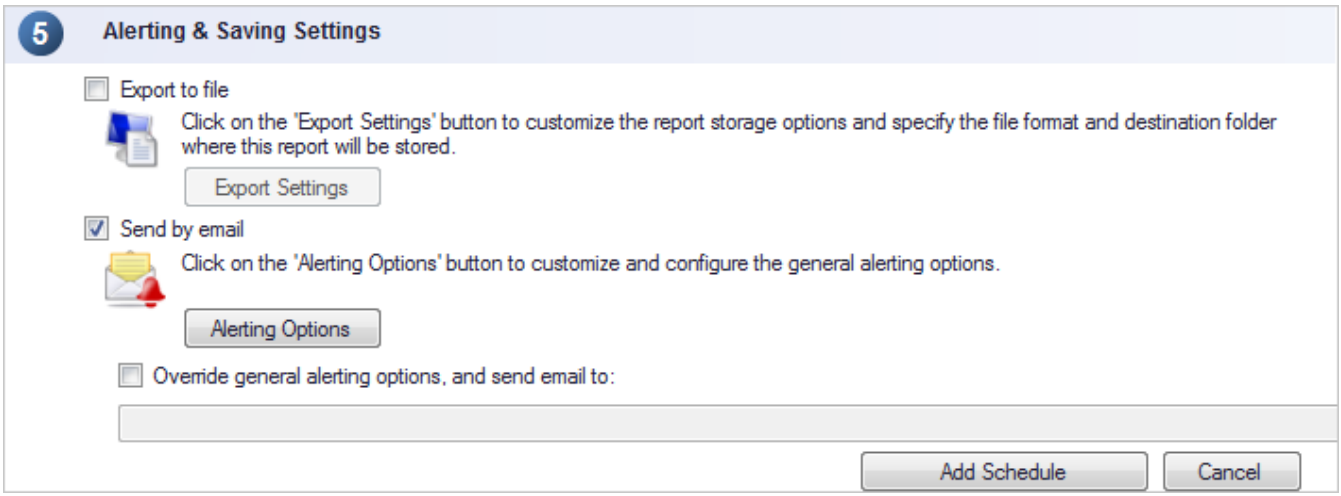
> **Nota**
>
> Ai rapporti pianificati è possibile applicare solo filtri personalizzati. For more information, refer to Utilizzo del Dashboard (page 86).



6. Da **Impostazioni di pianificazione**, configurare le seguenti opzioni:

Table 71: Opzioni di pianificazione

Opzione	Descrizione
Abilita pianificazione	Selezionare questa opzione per attivare la pianificazione e generare il rapporto in base alle impostazioni della pianificazione.
Solo una volta, il	Specificare la data e l'orario per la generazione del rapporto. Questa opzione genera il rapporto una volta, nella data specificata.
Schema di ricorrenza	Selezionare la frequenza di ricorrenza e indicare l'orario in cui generare il rapporto pianificato.


5
Alerting & Saving Settings
Export to file
Click on the 'Export Settings' button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Export Settings
Send by email
Click on the 'Alerting Options' button to customize and configure the general alerting options.
Alerting Options
Override general alerting options, and send email to:
Add Schedule
Cancel

7. Da **Impostazioni di avviso e di salvataggio**, configurare le seguenti opzioni:

Table 72: Impostazioni di avviso e di salvataggio

Opzione	Descrizione
Esporta su file	Selezionare questa opzione per salvare il rapporto in una cartella.
Impostazioni di esportazione	Fare clic su **Esporta impostazione** e dalla finestra di dialogo **Opzioni di archiviazione rapporti pianificati**, indicare la cartella in cui salvare il rapporto e il formato del rapporto salvato.
Invia per posta elettronica	Scegliere di inviare il rapporto per posta. Il rapporto viene inviato ai destinatari configurati nelle opzioni di avviso.
Opzioni di avviso	Fare clic su **Opzioni di avviso** e configurare i destinatari degli avvisi e le impostazioni del server di posta. For more information, refer to Configurazione delle opzioni di avviso (page 183).
Ignora opzioni generali di avviso e invia e-mail a	Selezionare di usare destinatari diversi da quelli configurati in Opzioni di avviso.

8. Per salvare il rapporto, fare clic su **Aggiungi pianificazione**.

Nota

10.3.2 Configurazione opzioni rapporti pianificati

Per configurare ulteriori impostazioni dei rapporti pianificati:

1. Dalla sezione **Rapporti pianificati** fare clic su **Opzioni rapporti pianificati**.

2. Per configurare le impostazioni dei messaggi di posta elettronica da utilizzare per l'invio di rapporto, fare clic su **Opzioni di avviso**. For more information, refer to Configurazione delle opzioni di avviso (page 183).

3. Per specificare il formato e il percorso di salvataggio dei rapporti generati, fare clic su **Opzioni di archiviazione**.

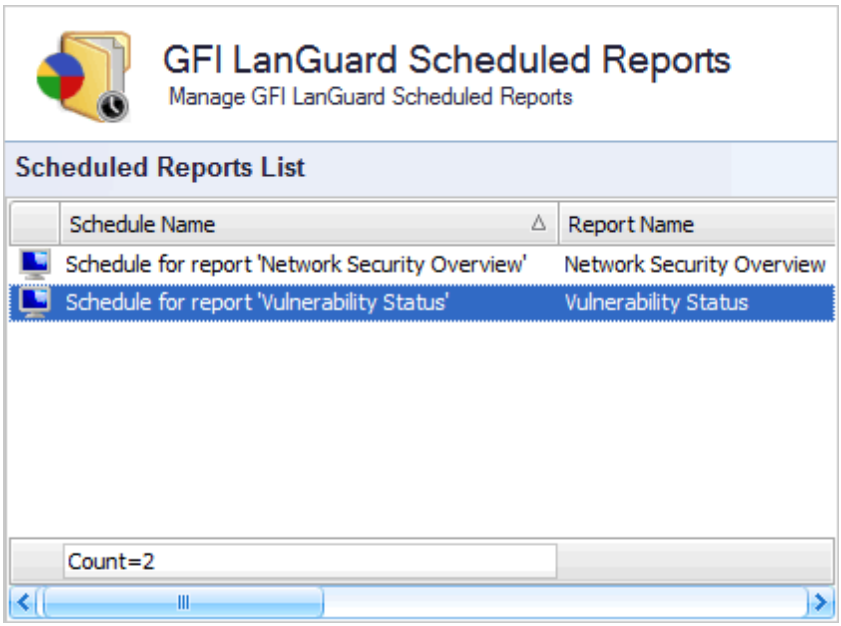
> **Nota**
>
> Per impostazione predefinita, tutti i rapporti generati vengono archiviati come `PDF` in: `<directory di installazione GFI LanGuard>\Reports`.

10.3.3 Gestione rapporti pianificati

Per gestire i rapporti pianificati:

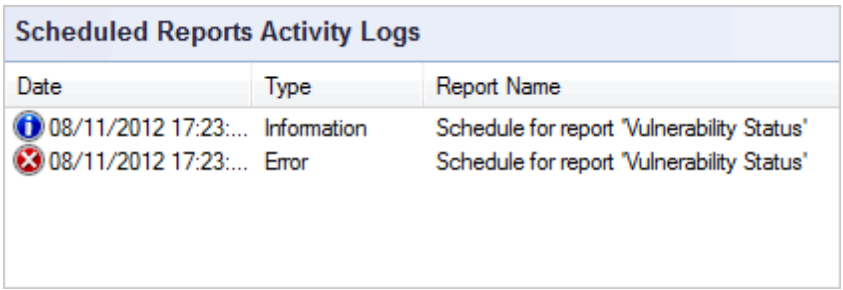
1. Fare clic sulla scheda **Rapporti**.

2. Da **Rapporti pianificati**, fare clic su **Elenco rapporti pianificati**.



Screenshot 111: Modifica opzioni rapporti pianificati

3. Per modificare le impostazioni del rapporto pianificato, fare doppio clic su un rapporto dal riquadro a destra.



Screenshot 112: Monitoraggio attività rapporti pianificati

4. L'attività dei rapporti pianificati può essere monitorata dalla sezione **Registri attività rapporti pianificati** posta in fondo al riquadro di destra.

10.4 Personalizzazione rapporti predefiniti

GFI LanGuard consente di creare nuovi rapporti sulla base delle impostazioni di un rapporto esistente. Questo consente un risparmio di tempo e semplifica l'ottimizzazione dei rapporti esistenti, in modo che il set di dati utilizzato per generare il rapporto sia il più adatto ai propri requisiti.

Questa sezione contiene informazioni relative a:

- Creazione rapporti personalizzati
- Personalizzazioni loghi rapporto
- Personalizzazione formato rapporto e-mail

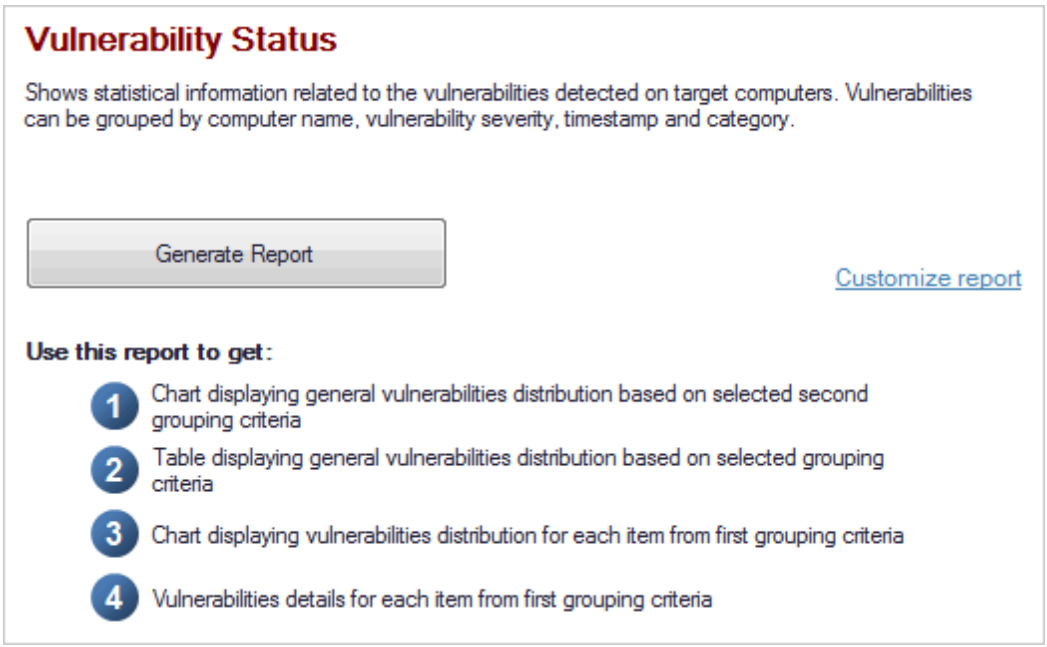
10.4.1 Creazione rapporti personalizzati

Per creare un rapporto personalizzato:

1. Fare clic sulla scheda **Rapporti**.

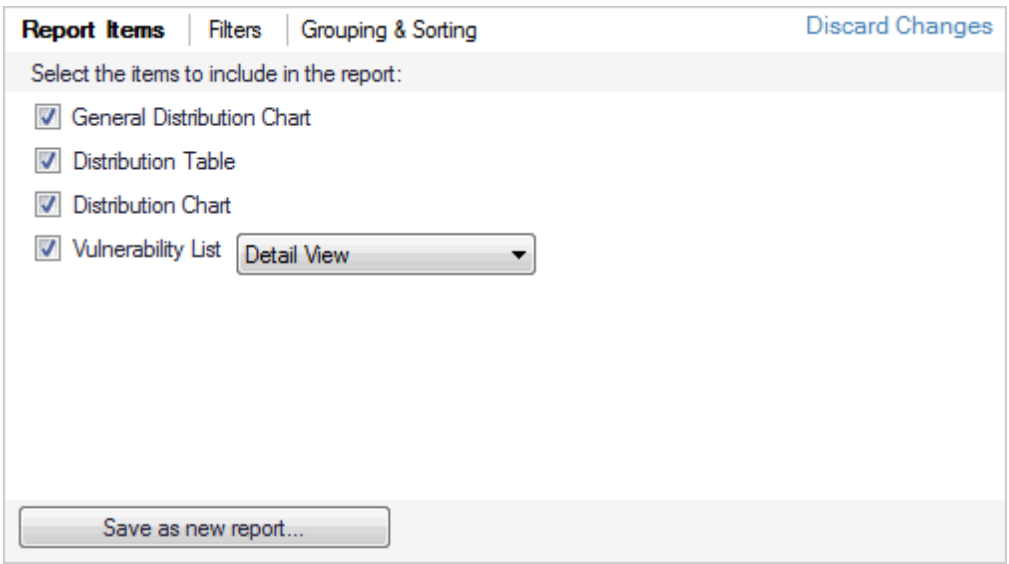
2. Dall'elenco **Rapporti**, selezionare un rapporto esistente, così da creare quelli nuovi sulla base delle relative impostazioni.

> **Nota**
>
> Non tutti i rapporti sono modificabili.


Vulnerability Status
Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.
Generate Report
Customize report
Use this report to get:
1 Chart displaying general vulnerabilities distribution based on selected second grouping criteria
2 Table displaying general vulnerabilities distribution based on selected grouping criteria
3 Chart displaying vulnerabilities distribution for each item from first grouping criteria
4 Vulnerabilities details for each item from first grouping criteria

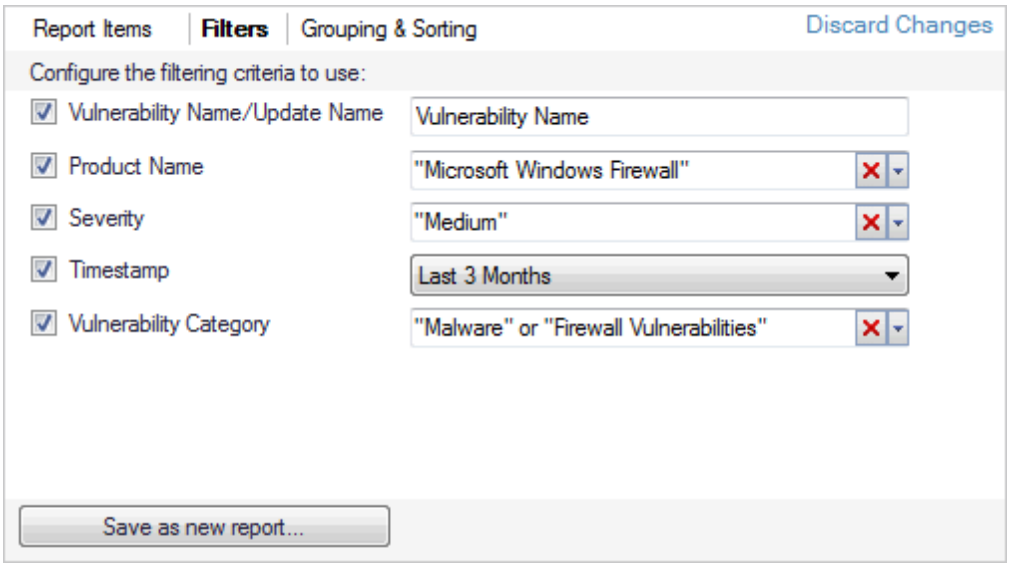
Screenshot 113: Modifica impostazioni rapporto dall'anteprima di esempio del rapporto

3. Dal riquadro a destra, selezionare **Personalizza rapporto** per visualizzare le opzioni avanzate del rapporto.



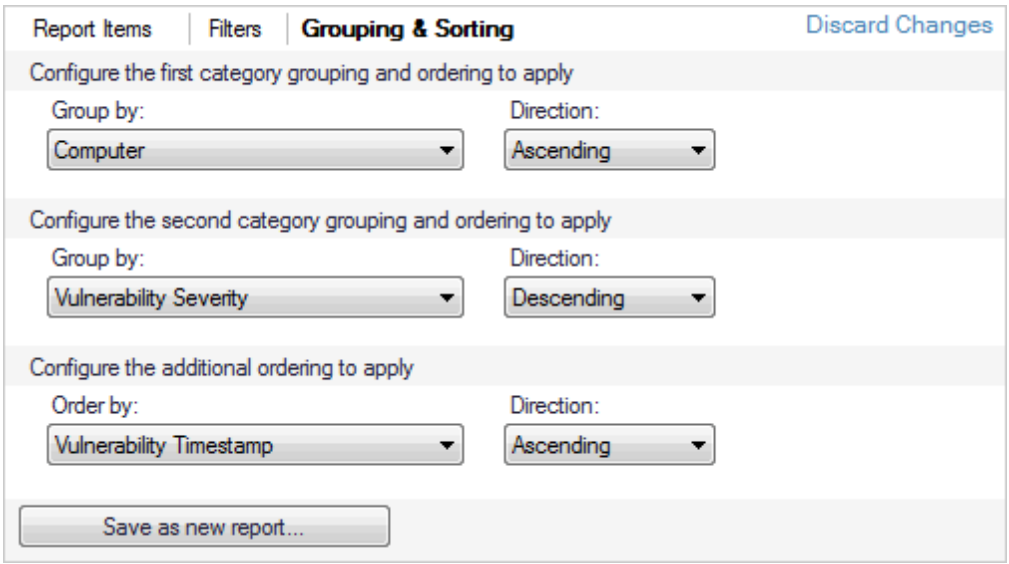
Screenshot 114: Configurazione elementi rapporto

4. Fare clic sulla scheda **Elementi rapporto** e selezionare gli elementi relativi da includere nel rapporto.



Screenshot 115: Configurazione opzioni filtro rapporto

5. Fare clic sulla scheda **Filtri** e configurare i filtri disponibili relativi al rapporto.



Screenshot 116: Configurazione opzioni di raggruppamento e ordinamento del rapporto

6. Fare clic sulla scheda **Raggruppamento e ordinamento**, quindi configurare:

- **Opzioni di raggruppamento**: le informazioni del rapporto sono raggruppate in base al campo selezionato.
- **Opzioni di raggruppamento seconda categoria**: le informazioni raggruppate vengono raggruppate in un sottogruppo in base al campo selezionato.
- **Ordinamento aggiuntivo**: ordinare le informazioni del rapporto in base al campo selezionato.

7. Fare clic su **Salva come nuovo rapporto...**.

8. Dalla finestra di dialogo **Aggiungi rapporto**, digitare un nome e una descrizione opzionale per il nuovo rapporto personalizzato. Fare clic su **OK**.

10.4.2 Personalizzazioni loghi rapporto

GFI LanGuard consente di utilizzare i loghi aziendali/personalizzati nei rapporti integrati presenti nel prodotto. I loghi possono essere collocati nelle sezioni dell'intestazione o del pié di pagina del

rapporto.

Personalizzazione logo intestazione rapporto

1. Creare/selezionare l'immagine.
2. Ridimensionare l'immagine a: Larghezza = **624**, Altezza = **25**.
3. Rinominare l'immagine in **headerlogo.png**.
4. Copiare/incollare l'immagine in `<directory di installazione GFI LanGuard>\Graphics\Logo`.

Personalizzazione logo pié di pagina rapporto

1. Creare/selezionare l'immagine.
2. Ridimensionare l'immagine a: Larghezza = **109**, Altezza = **41**.
3. Rinominare l'immagine in **footerlogo.png**.
4. Copiare/incollare l'immagine in `<directory di installazione GFI LanGuard>\Graphics\Logo`.

10.4.3 Personalizzazione formato rapporto e-mail

Per ciascun tipo di rapporto e-mail pianificato, vi è un file di formato predefinito HTML che include i segnaposto delimitati dal simbolo '%' (ad esempio: %TITLE%, %NAME%). È possibile modificare il formato HTML, modificare lo stile HTML, spostare ed eliminare i segnaposto per un'ulteriore personalizzazione del corpo del messaggio dei rapporti generati. Il percorso predefinito del modello è: `<directory di installazione GFI LanGuard> \ LanGuard 11 \ Templates \ template_mailbody.xml`.

GFI LanGuard può solo gestire i segnaposto noti (elencati di seguito) con il relativo ruolo predefinito. I segnaposto possono essere utilizzati in tutti i tipi di rapporti pianificati. La sottostante tabella illustra i segnaposto personalizzabili:

Table 73: Segnaposto rapporto

Segnaposto	Descrizione
%TITLE%	Titolo del messaggio di posta per il rapporto generato.
%NAME%	Nome rapporto pianificato.
%DESCRIPTION%:	Descrizione rapporto pianificato.
%TARGET%	Destinazioni (computer, domini) rappresentate nel rapporto pianificato.
%LAST_RUN%	Ultima data di esecuzione e ora del rapporto pianificato.
%NEXT_RUN%	Prossima data di esecuzione e ora del rapporto pianificato. **Nota** Questo segnaposto viene utilizzato esclusivamente per i rapporti digest giornalieri.
%PROFILE%	Profilo di scansione utilizzato durante l'esecuzione della scansione pianificata. **Nota** Questo segnaposto viene utilizzato esclusivamente per i rapporti di scansione a pianificazione posticipata.
%DURATION%	Durata scansione pianificata. **Nota** Questo segnaposto viene utilizzato esclusivamente per i rapporti di scansione a pianificazione posticipata.

Segnaposto	Descrizione
%ITEMS_COUNT%	Conteggio elementi raccolti. **Nota** Questo segnaposto viene utilizzato esclusivamente per i rapporti di scansione a pianificazione posticipata.
%AUTOREMED_ MISSINGPATCHES%	Utilizzato nel rapporto se è abilitata l'opzione di riparazione automatica patch mancanti per la scansione pianificata. **Nota** Questo segnaposto viene utilizzato esclusivamente per i rapporti di scansione a pianificazione posticipata.
%AUTOREMED_ MISSINGSPS%	Utilizzato nel rapporto se è abilitata l'opzione di riparazione automatica service pack mancanti per la scansione pianificata. **Nota** Questo segnaposto viene utilizzato esclusivamente per i rapporti di scansione a pianificazione posticipata.
%AUTOREMED_ UNINSTAPPS%	Utilizzato nel rapporto se è abilitata l'opzione di riparazione automatica di disinstallazione applicazioni per la scansione pianificata. **Nota** Questo segnaposto viene utilizzato esclusivamente per i rapporti di scansione a pianificazione posticipata.

10.5 Ricerca nel testo completo

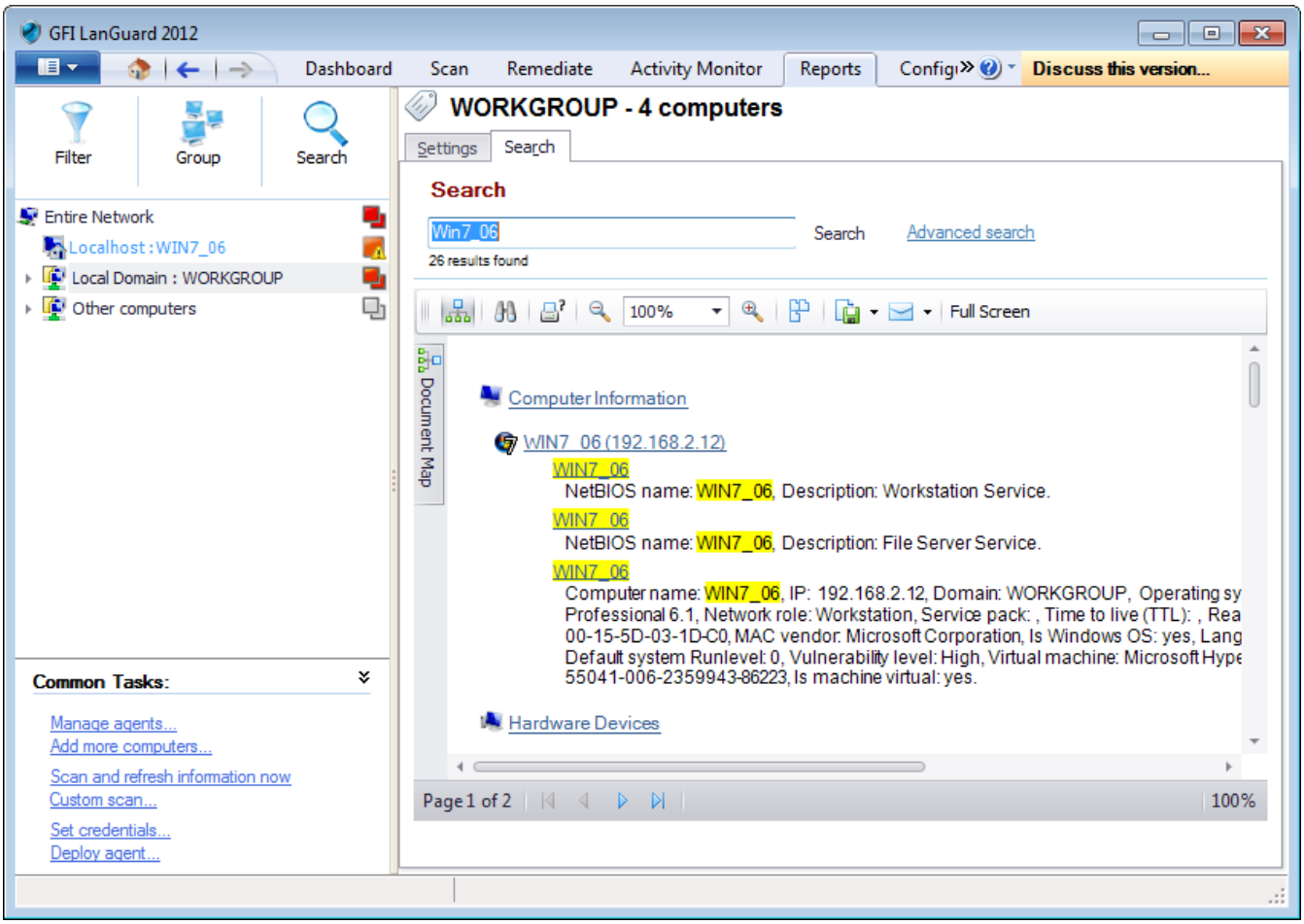
La funzionalità di ricerca nel testo completo restituisce i risultati in modo strutturato e configurabile. Qualsiasi risultato restituito offre collegamenti selezionabili, per visionare ulteriori dettagli.

Per utilizzare la funzionalità di ricerca nel testo completo:

1. Fare clic sulla scheda **Rapporti** sottoscheda **> Cerca**.

> **Nota**
>
> La ricerca è accessibile anche da **Struttura computer > Cerca**.

2. Immettere il termine da cercare, quindi fare clic su **Cerca**.

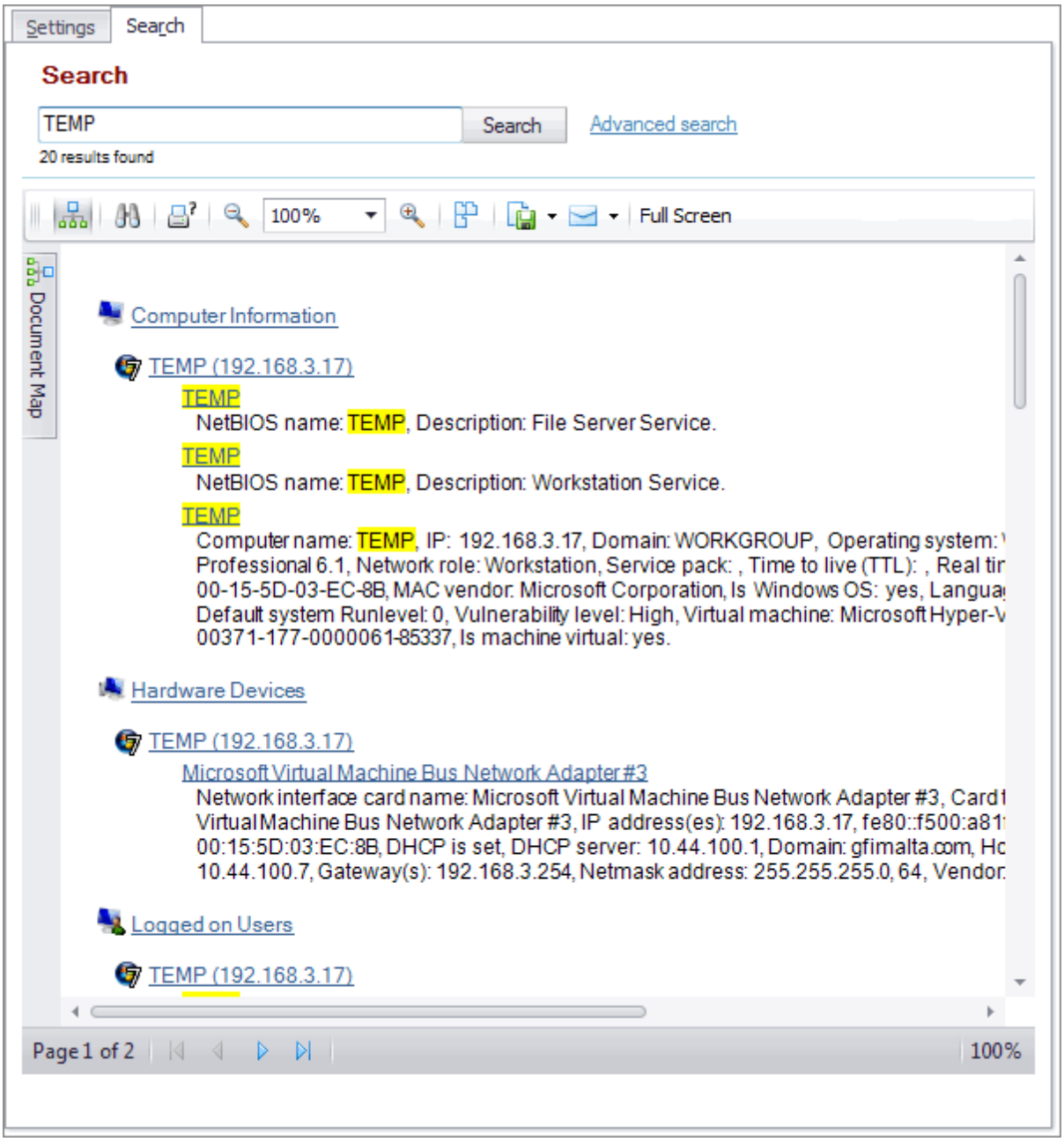


Screenshot 117: Personalizzazione dei parametri del rapporto

3. (Facoltativo) Per configurare i filtri che restringano la ricerca a qualcosa di più specifico, fare clic su **Ricerca avanzata**.

4. Analizzare i risultati di ricerca dalla sezione risultati collocata nella parte inferiore.

Il risultato contiene collegamenti che consentono di navigare tra computer, prodotti software e vulnerabilità. Ad esempio, è possibile fare clic sul collegamento di un service pack mancante per aprire le patch mancanti per un computer specifico.


Settings
Search
Search
TEMP
Search
Advanced search
20 results found
100%
Full Screen
Document Map
Computer Information
TEMP (192.168.3.17)
TEMP
NetBIOS name: TEMP, Description: File Server Service.
TEMP
NetBIOS name: TEMP, Description: Workstation Service.
TEMP
Computer name: TEMP, IP: 192.168.3.17, Domain: WORKGROUP, Operating system:
Professional 6.1, Network role: Workstation, Service pack: , Time to live (TTL): , Real tir
00-15-5D-03-EC-8B, MAC vendor: Microsoft Corporation, Is Windows OS: yes, Langua
Default system Runlevel: 0, Vulnerability level: High, Virtual machine: Microsoft Hyper-V
00371-177-0000061-85337, Is machine virtual: yes.
Hardware Devices
TEMP (192.168.3.17)
Microsoft Virtual Machine Bus Network Adapter #3
Network interface card name: Microsoft Virtual Machine Bus Network Adapter #3, Card1
Virtual Machine Bus Network Adapter #3, IP address(es): 192.168.3.17, fe80::f500:a81
00:15:5D:03:EC:8B, DHCP is set, DHCP server: 10.44.100.1, Domain: gfimalta.com, Hc
10.44.100.7, Gateway(s): 192.168.3.254, Netmask address: 255.255.255.0, 64, Vendor:
Logged on Users
TEMP (192.168.3.17)
Page 1 of 2
100%

Screenshot 118: Navigazione mediante i collegamenti dei rapporti

11 Personalizzazione di GFI LanGuard

La configurazione standard di GFI LanGuard consente di eseguire le scansioni di vulnerabilità utilizzando le impostazioni predefinite configurate in fabbrica. Se necessario, è anche possibile personalizzare queste impostazioni in modo da adattarle a qualsiasi particolare esigenza di gestione delle vulnerabilità della propria organizzazione. È possibile personalizzare e configurare vari aspetti di GFI LanGuard, incluse scansioni pianificate, controlli di vulnerabilità, filtri di scansione e profili di scansione.

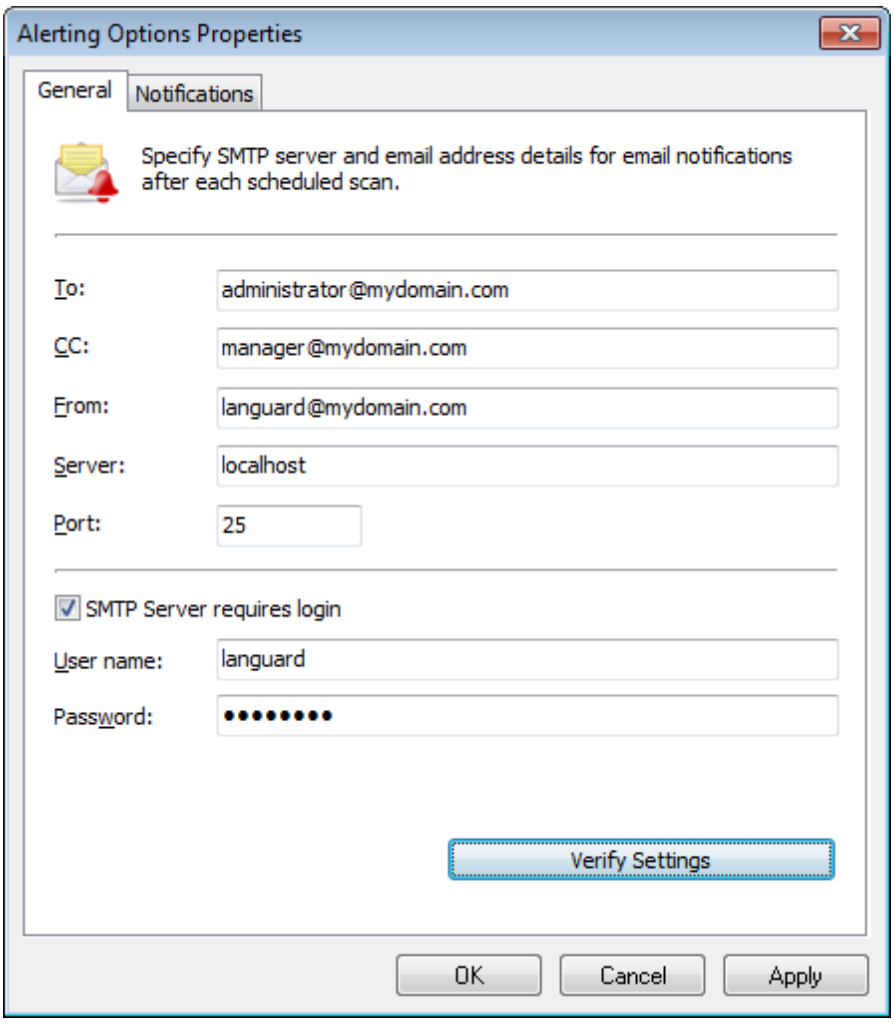
Argomenti del presente capitolo:

11.1 Configurazione delle opzioni di avviso 183
11.2 Configurazione opzioni di manutenzione database 184
11.3 Configurazione aggiornamenti del programma 190

11.1 Configurazione delle opzioni di avviso

Per configurare le opzioni di avviso:

1. Fare clic sulla scheda **Configurazione> Opzioni di avviso**.
2. Fare clic sul collegamento nel riquadro di destra.



Screenshot 119: Configurazione delle opzioni di avviso

3. Digitare i parametri descritti di seguito:

Table 74: Parametri impostazioni di posta

Opzione	Descrizione
A	L'indirizzo di posta elettronica del destinatario. Le e-mail inviate da GFI LanGuard vengono ricevute a questo indirizzo.
CC	Digitare un altro indirizzo di posta elettronica in questo campo, se è necessario inviare una copia a un altro indirizzo di posta.
Da	L'indirizzo di posta elettronica del mittente. GFI LanGuard utilizzerà questo account di posta per inviare i messaggi richiesti.
Server	Definisce il server attraverso cui vengono instradati i messaggi. Può essere un FQDN (Fully Qualified Domain Name) o un indirizzo IP.
Porta	Definisce la porta IP attraverso cui vengono instradati i messaggi. Il valore predefinito è 25
Il server SMTP richiede l'accesso	Se il server SMTP richiede un nome utente e una password per l'autenticazione, selezionare questa opzione.

4. Fare clic sul pulsante **Verifica impostazioni** per verificare le impostazioni di posta elettronica.

5. Selezionare **Notifiche** e configurare le seguenti opzioni:

Table 75: Opzioni di notifica

Opzione	Descrizione
Attiva digest giornaliero	Ricezione di rapporti giornalieri con tutte le modifiche effettuate sull'intera rete. Configurare l'orario in cui ricevere il messaggio del digest giornaliero.
Formato rapporto	Specificare il formato del rapporto ricevuto per posta elettronica.
Invia un'e-mail su novità nuovi prodotti	Per ricevere un'e-mail contenente le novità sui nuovi prodotti.

6. Fare clic su **OK**.

11.2 Configurazione opzioni di manutenzione database

GFI LanGuard viene fornito con un insieme di opzioni per la manutenzione del database che può essere usato per una buona manutenzione del database back-end relativo ai risultati di scansione.

Ad esempio, è possibile migliorare le prestazioni del prodotto e impedire che il database back-end dei risultati di scansione diventi eccessivamente voluminoso eliminando automaticamente i risultati di scansione più vecchi di un determinato numero di mesi.

Se si utilizza un database back-end Access™, è anche possibile pianificare la compattazione del database. La compattazione permette di riparare i dati danneggiati e di eliminare i registri del database contrassegnati per l'eliminazione all'interno del backend del database, assicurando così l'integrità del database dei risultati della scansione. Nelle sezioni seguenti vengono fornite le informazioni su:

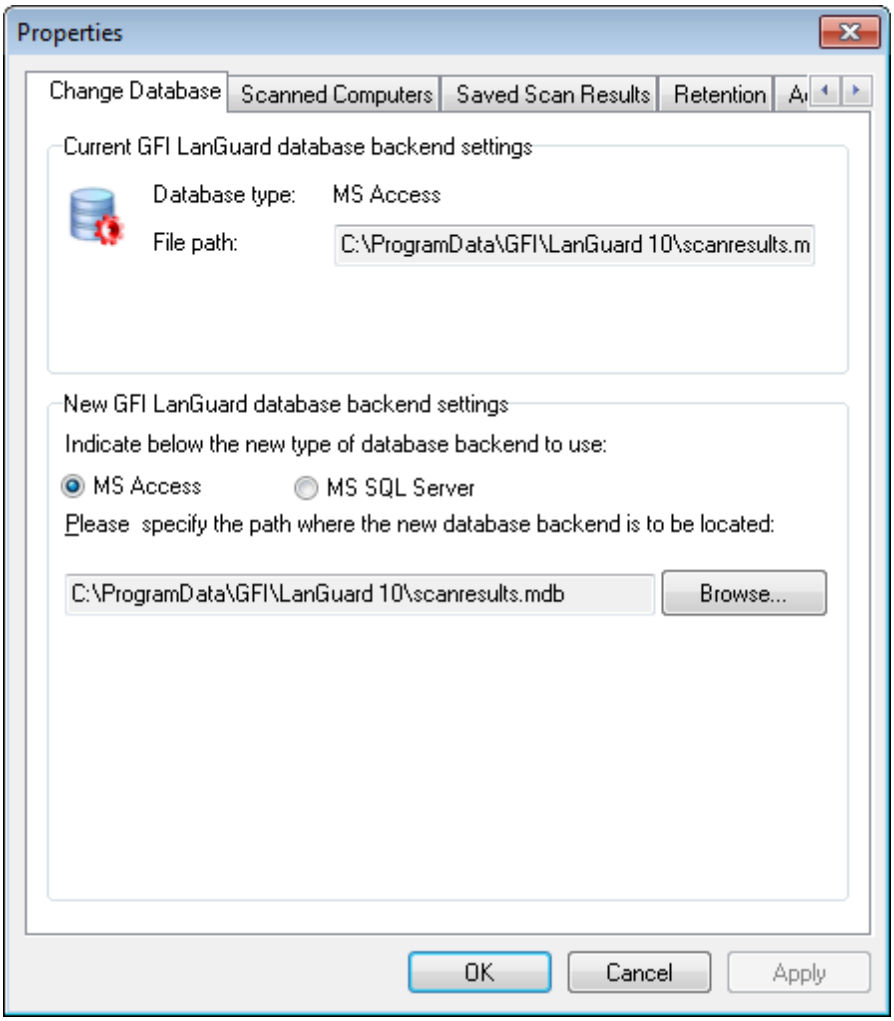
- Utilizzo di Access™ come database back-end
- Utilizzo di SQL Server® come database back-end
- Gestione dei risultati della scansione salvati
- Elenco dei computer sottoposti a scansione
- Configurazione opzioni di manutenzione database avanzate
- Configurazione delle opzioni di conservazione database

11.2.1 Utilizzo di Access™ come database back-end

GFI LanGuard supporta i database back-end basati su Access™ e SQL Server® (2000 o successivo).

Per memorizzare i risultati della scansione in un database Access™:

1. Fare clic sulla scheda **Configurazione> Opzioni di manutenzione database > Impostazioni back-end database**.



Screenshot 120: Finestra di dialogo Proprietà di manutenzione del database

2. Selezionare l'opzione **MS Access** e specificare il percorso completo (compreso il nome del file) del database back-end Access™.

Nota

Se il file del database specificato non esiste, verrà creato.

Nota

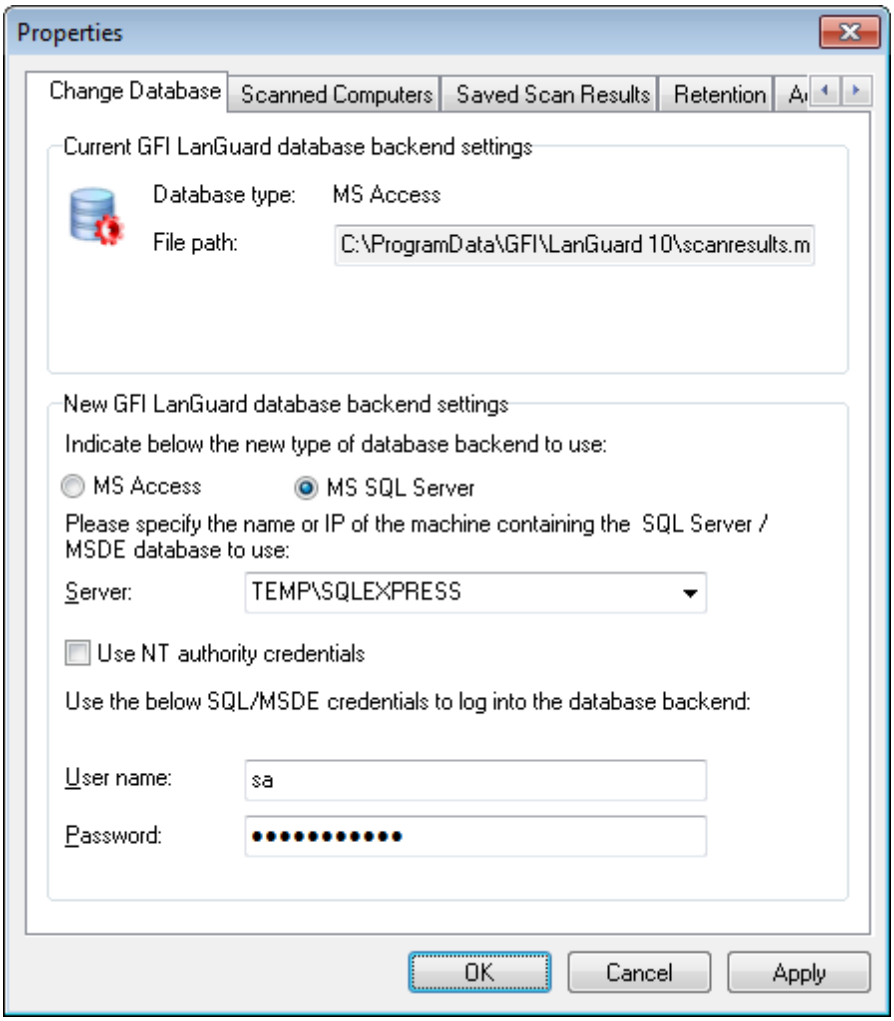
Se il file del database specificato esiste già e appartiene a una versione precedente di GFI LanGuard, il sistema chiederà all'utente di sovrascrivere le informazioni esistenti.

3. Fare clic su **OK**.

11.2.2 Utilizzo di SQL Server® come database back-end

Per memorizzare i risultati della scansione in un database SQL Server®:

1. Fare clic sulla scheda **Configurazione> Opzioni di manutenzione database > Impostazioni back-end database.**



Screenshot 121: Opzioni database back-end SQL Server®

2. Selezionare l'opzione **MS Server SQL** e dall'elenco dei server rilevati sulla rete, scegliere il server SQL Server sul quale sarà ospitato il database.

3. Specificare le credenziali del server SQL Server o selezionare l'opzione **Usa credenziali di autorizzazione NT** per autenticare il server SQL Server utilizzando i dettagli dell'account Windows.

4. Fare clic su **OK** per completare le impostazioni in uso.

Nota

Se il server e le credenziali specificati sono corretti, GFI LanGuard effettuerà automaticamente l'accesso al server SQL Server e creerà le tabelle database necessarie. Se le tabelle del database esistono già, GFI LanGuard le riutilizzerà.

Nota

Quando si utilizzano le credenziali di autorizzazione NT, assicurarsi che i servizi di GFI LanGuard vengano eseguiti all'interno di un account dotato di privilegi di accesso e amministrativi sui database del server SQL Server.

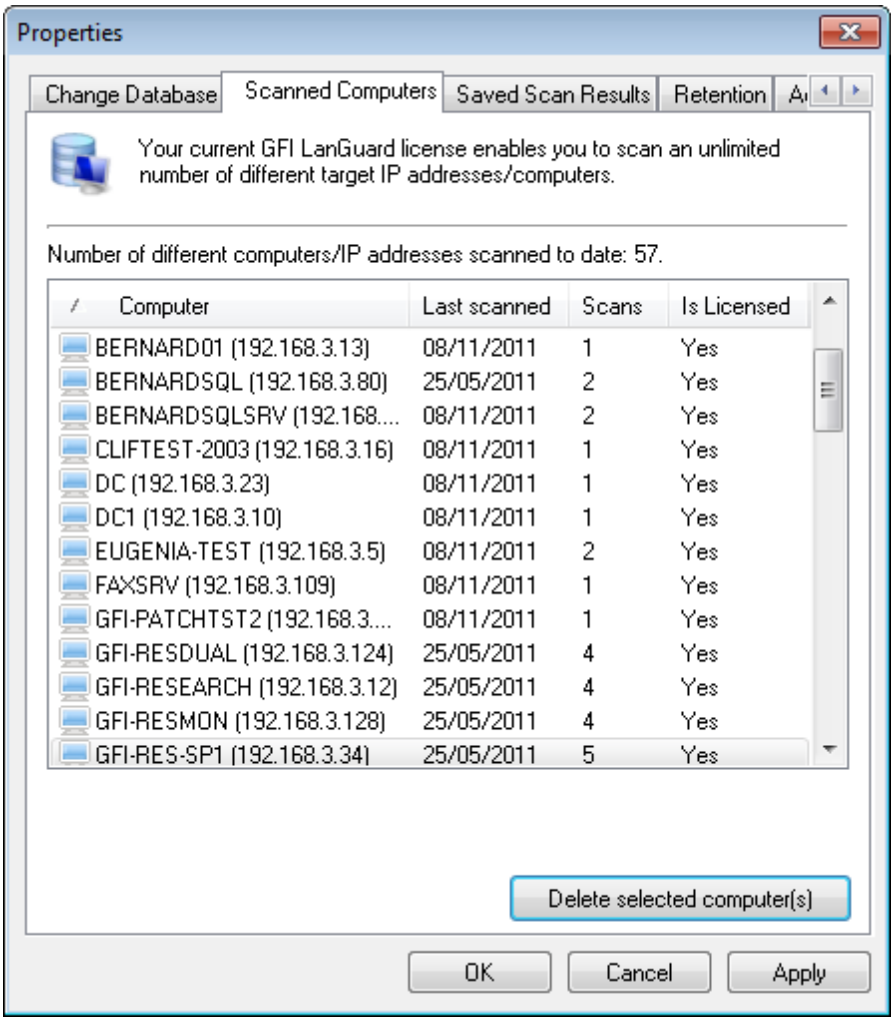
5. Per interrompere tutte le scansioni in esecuzione, fare clic su **Sì**.

6. Se il database Access™ corrente contiene dati, fare clic su **OK** per trasferire tutti i dati di scansione al database SQL Server®.

11.2.3 Gestione dei risultati della scansione salvati

Usare la scheda **Risultati della scansione salvati** per gestire il database back-end ed eliminare i risultati scansione salvati non più necessari. L'eliminazione dei risultati della scansione salvati non necessari può essere eseguita manualmente o automaticamente tramite la manutenzione pianificata del database.

Durante la manutenzione pianificata del database, GFI LanGuard elimina automaticamente i risultati della scansione salvati che sono più vecchi di un determinato numero di giorni/settimane o mesi. È anche possibile configurare la manutenzione automatica del database di modo che conservi solo un determinato numero di risultati recenti della scansione per ciascuna destinazione e ciascun profilo di scansione.


Properties
Change Database
Scanned Computers
Saved Scan Results
Retention
Your current GFI LanGuard license enables you to scan an unlimited number of different target IP addresses/computers.
Number of different computers/IP addresses scanned to date: 57.
Computer
Last scanned
Scans
Is Licensed
BERNARD01 (192.168.3.13) 08/11/2011 1 Yes
BERNARDSQL (192.168.3.80) 25/05/2011 2 Yes
BERNARDSQLSRV (192.168.... 08/11/2011 2 Yes
CLIFTEST-2003 (192.168.3.16) 08/11/2011 1 Yes
DC (192.168.3.23) 08/11/2011 1 Yes
DC1 (192.168.3.10) 08/11/2011 1 Yes
EUGENIA-TEST (192.168.3.5) 08/11/2011 2 Yes
FAXSRV (192.168.3.109) 08/11/2011 1 Yes
GFI-PATCHTST2 (192.168.3.... 08/11/2011 1 Yes
GFI-RESDUAL (192.168.3.124) 25/05/2011 4 Yes
GFI-RESEARCH (192.168.3.12) 25/05/2011 4 Yes
GFI-RESMON (192.168.3.128) 25/05/2011 4 Yes
GFI-RES-SP1 (192.168.3.34) 25/05/2011 5 Yes
Delete selected computer(s)
OK
Cancel
Apply

Screenshot 122: Proprietà manutenzione del database: scheda Gestisci risultati della scansione salvati

Per gestire i risultati della scansione salvati:

1. Fare clic sulla scheda **Configurazione> Opzioni di manutenzione database > Gestisci risultati della scansione salvati**.

2. Per eliminare i risultati della scansione salvati, scegliere il risultato desiderato e fare clic su **Elimina scansione/i**.

3. Per lasciare a GFI LanGuard il compito di gestire il database, selezionare **Scansioni generate durante l'ultimo** per eliminare automaticamente i risultati della scansione più vecchi di un determinato numero di giorni/settimane o mesi o **Esegui scansione per destinazione di scansione per profilo nel numero di** per conservare solo un determinato numero di risultati recenti della scansione.

11.2.4 Elenco dei computer sottoposti a scansione

GFI LanGuardAi fini dell'utilizzo in licenza, gestisce un elenco globale di computer sottoposti a scansione. Non verrà eseguita la scansione dei computer non compresi nelle informazioni della licenza.

GFI LanGuard consente agli amministratori di sistema di eliminare i computer scansionati in modo da rilasciare le licenze precedentemente utilizzate.

Per eliminare i computer precedentemente sottoposti a scansione:

1. Selezionare la scheda **Configurazione** scheda **> Opzioni di manutenzione database > Gestisci elenco dei computer sottoposti a scansione**.

2. Selezionare i computer da eliminare e fare clic su **Elimina computer selezionato/i**.

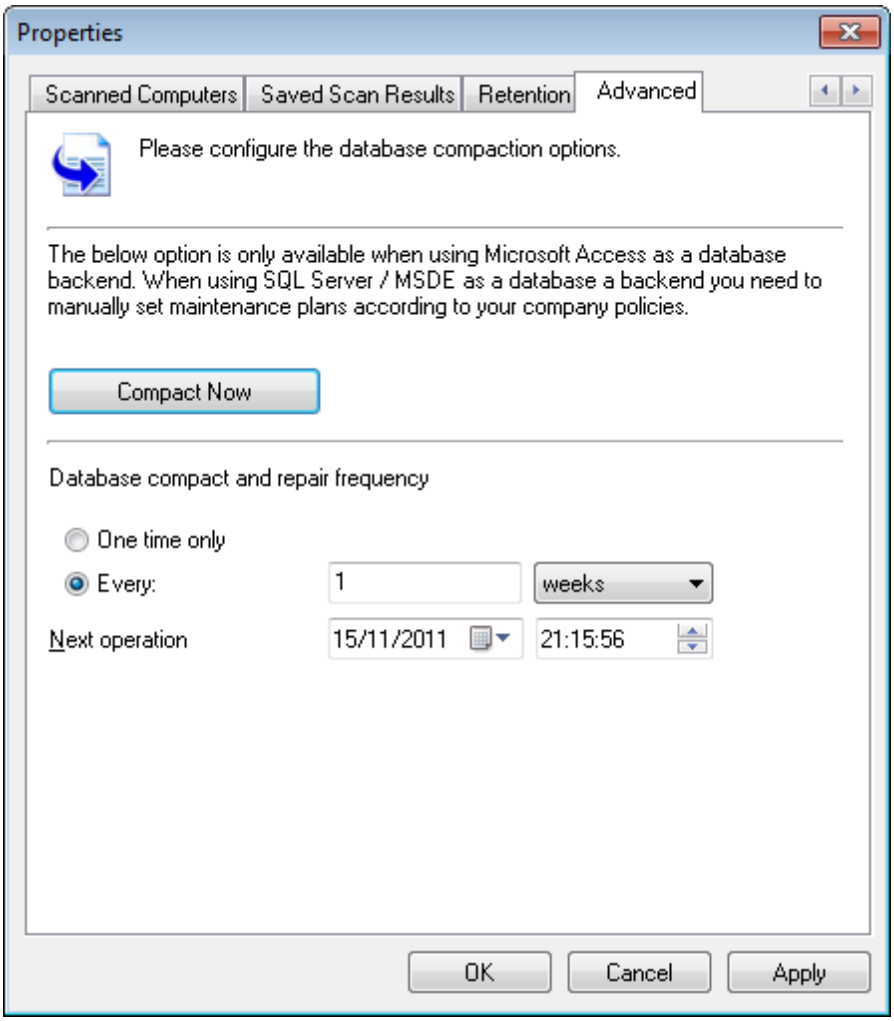
IMPORTANTE

L'eliminazione dei computer dal database è un'operazione irreversibile che eliminerà dal database anche tutti i dati relativi al computer. Una volta eliminati, questi dati non sono più disponibili.

11.2.5 Configurazione opzioni di manutenzione database avanzate

GFI LanGuard consente di correggere e compattare automaticamente il database back-end Access™ per migliorare le prestazioni.

Durante la compattazione i file del database vengono organizzati e i registri contrassegnati per l'eliminazione vengono rimossi. In questo modo è possibile recuperare spazio di archiviazione in uso. Durante questo processo, GFI LanGuard ripara inoltre i file danneggiati del database back-end. Il danneggiamento dei file può essere dovuto a varie ragioni. Nella maggior parte dei casi, un database Access™ risulta danneggiato quando viene chiuso in modo imprevisto prima che i registri siano stati salvati (ad esempio a causa di un calo di corrente, riavvii forzati di operazioni che non rispondono, ecc.).



Screenshot 123: Proprietà manutenzione del database: scheda Avanzate

Per compattare e riparare un database back-end Access™:

1. Fare clic sulla scheda **Configurazione> Opzioni di manutenzione database > Piano di manutenzione database**.

2. Per avviare manualmente un processo di riparazione e compattazione su un vecchio database back-end Access™, fare clic sul pulsante **Compatta ora**.

3. Per automatizzare il processo di riparazione e compattazione sul database del back-end Access™, selezionare:

- **Solo una volta**: per pianificare un'unica esecuzione della riparazione e della compattazione del database Access™
- **Ogni**: per eseguire il processo di riparazione e compattazione in base a una pianificazione regolare.

Specificare la data, l'ora e la frequenza in giorni/settimane o mesi con la quale eseguire le operazioni di compattazione e riparazione sul database back-end.

11.2.6 Configurazione delle opzioni di conservazione database

Le opzioni di conservazione del database consentono di mantenere il database pulito e coerente configurando GFI LanGuard per l'eliminazione automatica dei risultati di scansione indesiderati e delle informazioni della cronologia di scansione, pur conservando quelli importanti.

Per configurare le impostazioni di conservazione:

1. Fare clic sulla scheda **Configurazione> Opzioni di manutenzione database > Impostazioni back-end database scheda > Conservazione**.

2. Configurare le opzioni descritte di seguito:

Table 76: Opzioni di conservazione database

Opzione	Descrizione
Conserva scansioni generate negli ultimi	Conserva i risultati di scansione generati nel numero di giorni/settimane/mesi specificato.
Numero di scansioni da conservare per destinazione di scansione e per profilo	Specifica il numero di risultati di scansione da conservare per ciascuna destinazione di scansione e per ogni profilo di scansione.
Non eliminare mai cronologia	Scegliere questa opzione per mantenere l'intera cronologia di scansione.
Conserva cronologia per	Conserva la cronologia di scansione per il numero specificato di giorni/settimane/mesi.

3. Fare clic su **OK**.

11.3 Configurazione aggiornamenti del programma

Questo strumento consente a GFI LanGuard di rilevare le ultime vulnerabilità e mantenere le prestazioni di scansione. Configurare GFI LanGuard affinché scarichi automaticamente gli aggiornamenti rilasciati da GFI al fine di migliorare le funzionalità di GFI LanGuard. Tali aggiornamenti comprendono anche il controllo del sito Web di GFI per verificare la presenza di build più recenti. Gli aggiornamenti possono essere abilitati/disabilitati selezionando la casella di controllo nella colonna **Download automatico**.

GFI LanGuard può eseguire il download di tutte le lingue Unicode. Ciò comprende (ma non esclusivamente) inglese, tedesco, francese, italiano, spagnolo, arabo, danese, ceco, finlandese, ebraico, ungherese, giapponese, coreano, olandese, norvegese, polacco, portoghese, portoghese/brasiliano, russo, svedese, cinese, cinese (Taiwan), greco e turco.

Nelle sezioni seguenti vengono fornite le informazioni su:

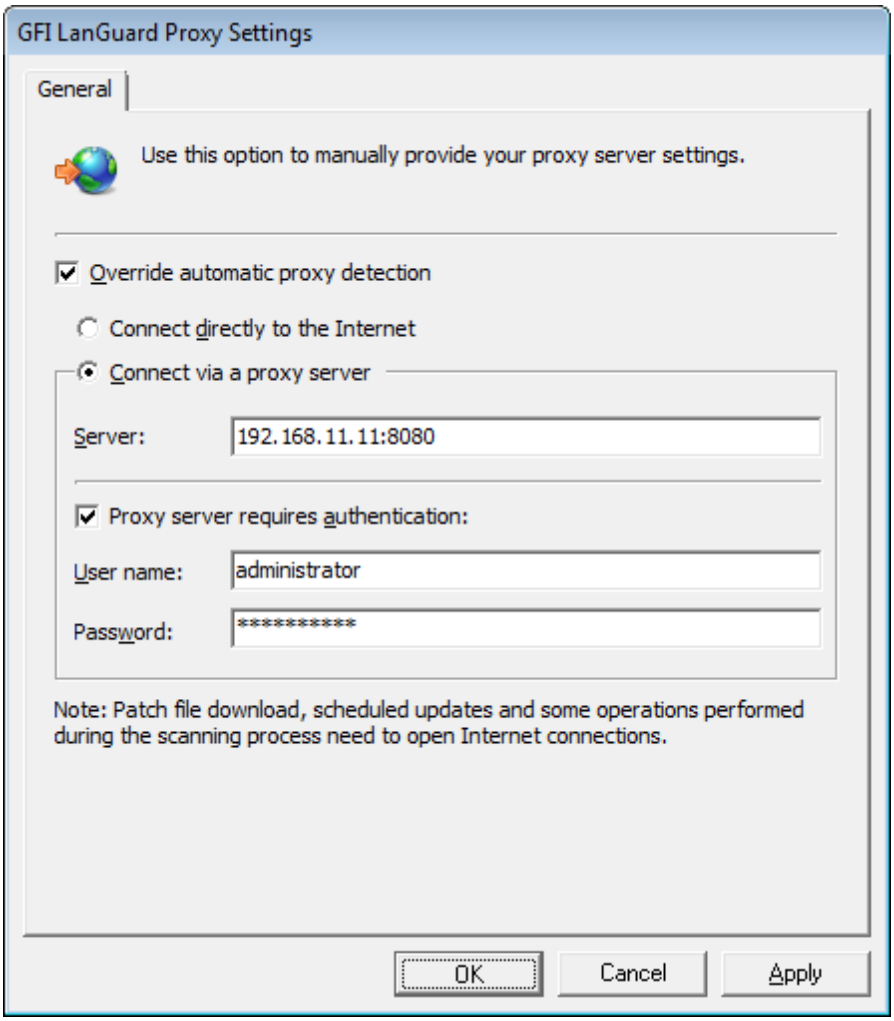
- Configurazione impostazioni proxy
- Configurazione opzioni di aggiornamento automatico
- Installazione manuale degli aggiornamenti del programma

11.3.1 Configurazione impostazioni proxy

Per configurare manualmente le impostazioni del server proxy per gli aggiornamenti Internet:

1. Fare clic sulla scheda **Configurazione> Aggiornamenti del programma**.

2. Da **Attività comuni**, fare clic su **Modifica impostazioni proxy**.



Screenshot 124: Configurazione delle impostazioni del server proxy

3. Selezionare **Ignora rilevamento automatico del proxy;** configurare le opzioni descritte di seguito:

Table 77: Impostazioni proxy

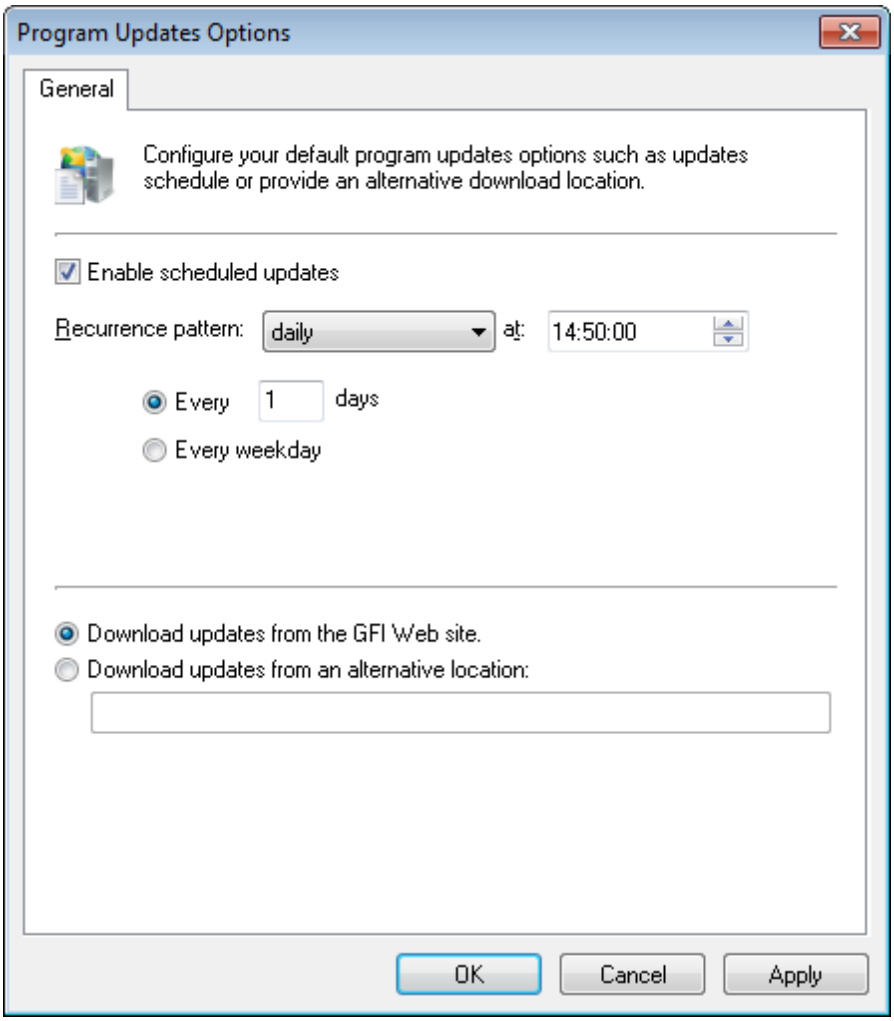
Opzione	Descrizione
Connetti direttamente a Internet	È disponibile una connessione diretta a Internet.
Connetti tramite un server proxy	L'accesso a Internet avviene tramite un server proxy. Aggiornare il nome del Server e il numero della porta utilizzando questo formato <server>:<porta>
Il server proxy richiede l'autenticazione	(Facoltativo) Immettere nome utente e password, se richiesto dal server proxy.

4. Fare clic su **OK**.

11.3.2 Configurazione opzioni di aggiornamento automatico

GFI LanGuard consente di verificare la disponibilità di aggiornamenti software a ogni avvio del programma. Per abilitare/disabilitare questa funzionalità:

1. Fare clic sulla scheda **Configurazione> Aggiornamenti del programma**. In **Attività comuni** selezionare **Modifica opzioni di aggiornamento programma**.



Screenshot 125: Configurazione aggiornamenti all'avvio dell'applicazione

2. Per abilitare/disabilitare i controlli automatici degli aggiornamenti all'avvio dell'applicazione, selezionare/deselezionare **Verifica la disponibilità di aggiornamenti all'avvio dell'applicazione**.

3. Selezionare/deselezionare Attiva aggiornamenti pianificati per configurare la frequenza dei controlli degli aggiornamenti.

4. Specificare se GFI LanGuard scarica gli aggiornamenti dal sito Web GFI o da un percorso alternativo.

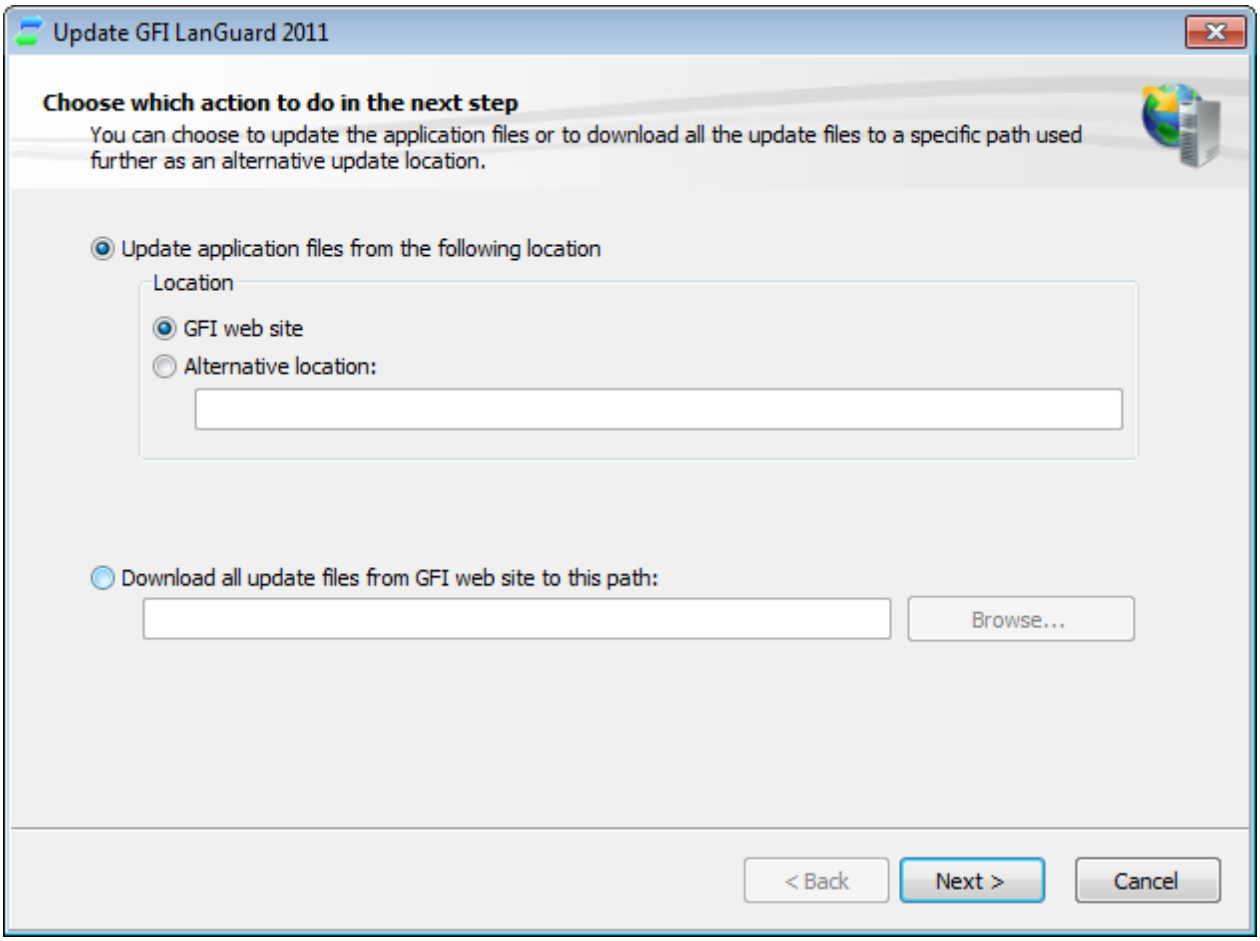
5. Fare clic su **OK**.

11.3.3 Installazione manuale degli aggiornamenti del programma

Per avviare manualmente gli aggiornamenti del programma GFI LanGuard:

1. Fare clic sulla scheda **Configurazione> Aggiornamenti del programma**.

2. In **Attività comuni**, selezionare **Verifica disponibilità aggiornamenti**.


Update GFI LanGuard 2011
Choose which action to do in the next step
You can choose to update the application files or to download all the update files to a specific path used further as an alternative update location.
Update application files from the following location
Location
GFI web site
Alternative location:
Download all update files from GFI web site to this path:
Browse...
< Back
Next >
Cancel

Screenshot 126: Procedura guidata Verifica disponibilità aggiornamenti

3. Specificare la posizione dalla quale scaricare i file di aggiornamento necessari.

4. (Facoltativo) Modificare il percorso di download predefinito selezionando l'opzione **Scarica tutti i file di aggiornamento...** in questo percorso per specificare un percorso di download alternativo in cui salvare tutti gli aggiornamenti di GFI LanGuard.

5. Fare clic su **Avanti** per procedere con l'aggiornamento.

6. Selezionare gli aggiornamenti e fare clic su **Avanti**.

7. Fare clic su **Avvia** per avviare il processo di aggiornamento.

12 Editor dei profili di scansione

I profili di scansione forniti con GFI LanGuard sono stati preconfigurati per l'esecuzione di una serie di controlli di vulnerabilità sulla destinazione selezionata. È possibile tuttavia disabilitare le scansioni delle vulnerabilità e personalizzare l'elenco dei controlli di vulnerabilità eseguiti durante una scansione. Le scansioni possono essere modificate tramite l'**Editor del profilo di scansione**.

Argomenti del presente capitolo:

12.1 Creazione di un nuovo profilo di scansione 194
12.2 Configurazione delle vulnerabilità 195
12.3 Configurazione delle patch 205
12.4 Configurazione opzioni di controllo rete e software 208
12.5 Configurazione delle opzioni di scansione di sicurezza 217

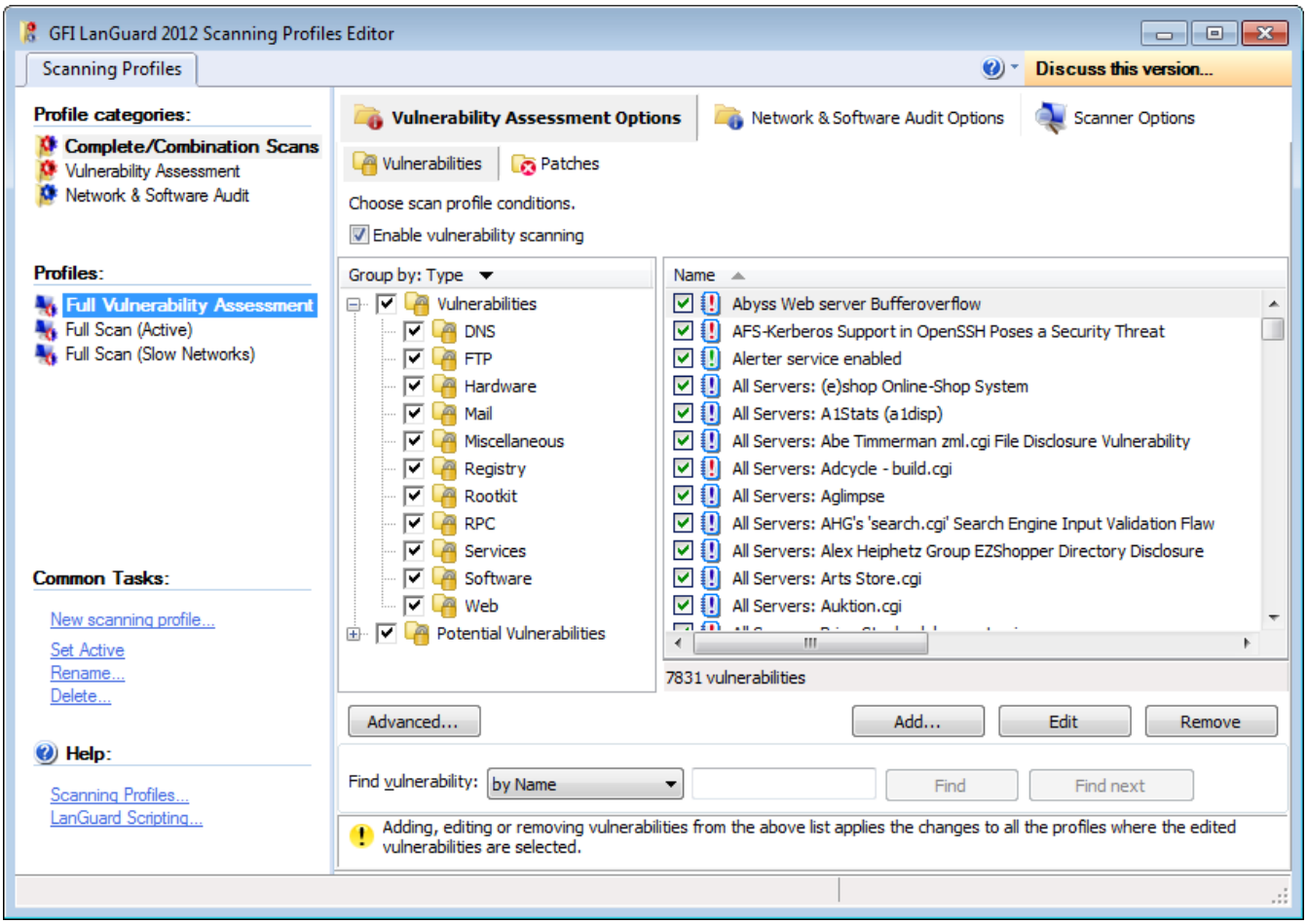
12.1 Creazione di un nuovo profilo di scansione

Editor dei profili di scansione consente di creare nuovi profili di scansione. Per creare un nuovo profilo di scansione personalizzato:

1. Avviare GFI LanGuard.

2. Fare clic sul pulsante GFI LanGuard e selezionare **Configurazione > Editor dei profili di scansione**. In alternativa, premere **CTRL + P** per avviare l'**Editor profili di scansione**.

3. Nell'**Editor dei profili di scansione**, in **Attività comuni**, selezionare **Nuovo profilo di scansione**.



Screenshot 127: Editor del profilo di scansione

4. Specificare il nome del nuovo profilo ed eventualmente selezionare **Copia tutte le impostazioni da un profilo esistente** per clonare le impostazioni di un profilo esistente.

5. Fare clic su **OK** per salvare le impostazioni. Il nuovo profilo di scansione viene aggiunto sotto **Profili** nel riquadro di sinistra.

12.2 Configurazione delle vulnerabilità

La scheda **Opzioni di valutazione delle vulnerabilità** consente di configurare gli aggiornamenti Microsoft®/non Microsoft® e di sicurezza/non di sicurezza selezionati quando si esegue la scansione delle destinazioni con il profilo selezionato.

Nelle sezioni seguenti vengono fornite le informazioni su:

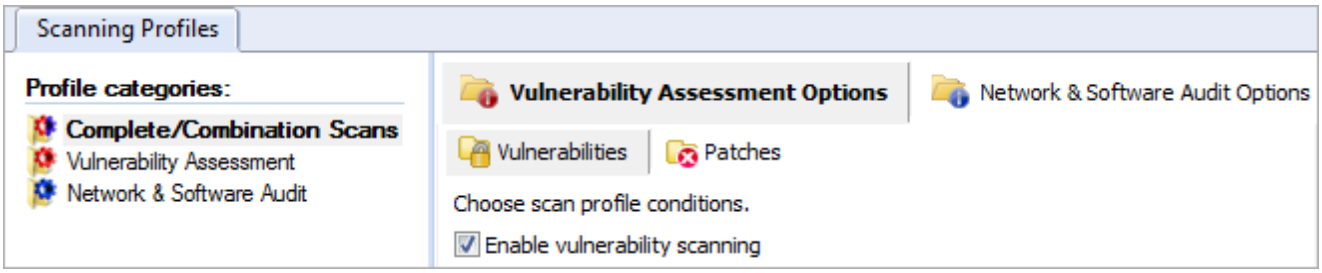
- Abilitazione della scansione di vulnerabilità
- Personalizzazione dell'elenco delle vulnerabilità da sottoporre a scansione
- Personalizzazione proprietà controlli di vulnerabilità
- Configurazione delle condizioni dei controlli di vulnerabilità

12.2.1 Abilitazione della scansione di vulnerabilità

Per abilitare la scansione delle vulnerabilità:

1. Avviare GFI LanGuard.

2. Fare clic sul pulsante GFI LanGuard e selezionare **Configurazione > Editor dei profili di scansione**. In alternativa, premere **CTRL + P** per avviare l'**Editor profili di scansione**.



Screenshot 128: Abilitazione della scansione di vulnerabilità per il profilo di scansione selezionato

3. Nella scheda **Opzioni di valutazione delle vulnerabilità** fare clic sulla sottoscheda **Vulnerabilità**.

4. Selezionare il profilo di scansione da personalizzare dal riquadro di sinistra sotto **Profili**.

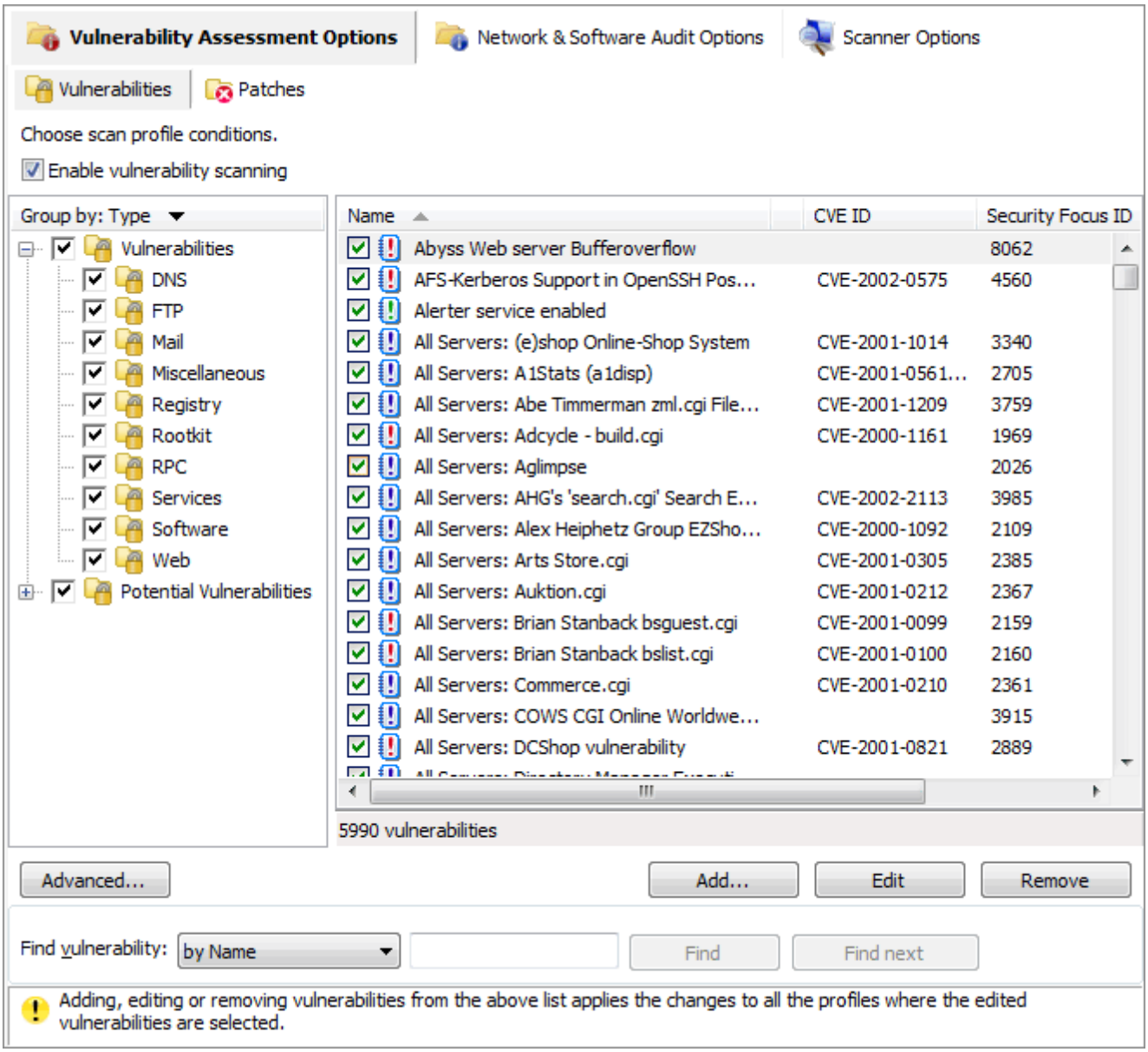
5. Nel riquadro di destra selezionare **Abilita scansione delle vulnerabilità**.

> **Nota**
>
> La scansione delle vulnerabilità viene configurata in un profilo di scansione in modo specifico per quel profilo. Se questa opzione non è selezionata in un particolare profilo, non verrà eseguito alcun test delle vulnerabilità nell'ambito dei controlli di sicurezza eseguiti da questo profilo di scansione.

12.2.2 Personalizzazione dell'elenco delle vulnerabilità da sottoporre a scansione

Per specificare le vulnerabilità che il profilo di scansione dovrà enumerare ed elaborare durante un controllo di protezione:

1. Dalla scheda **Opzioni di valutazione delle vulnerabilità**, selezionare il profilo di scansione da personalizzare nel riquadro di sinistra sotto **Profili**.

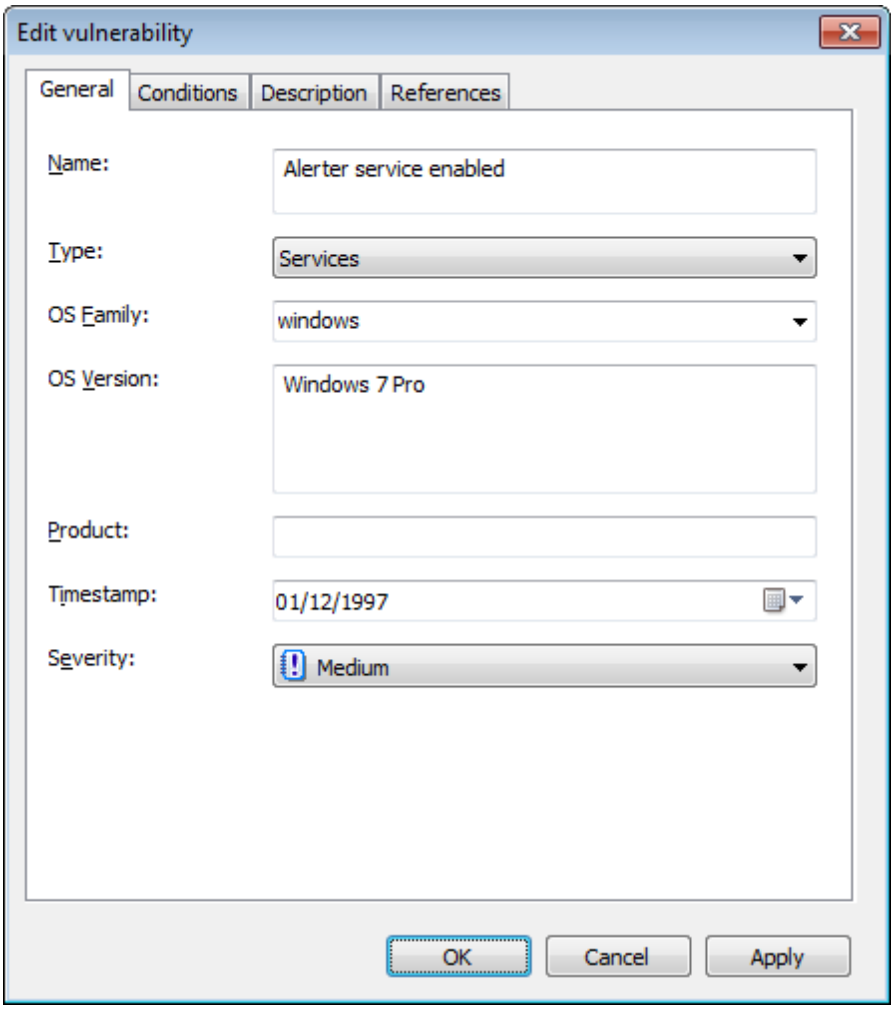


Screenshot 129: Selezionare i controlli di vulnerabilità eseguiti da questo profilo di scansione

2. Nel riquadro di destra, selezionare i controlli di vulnerabilità da eseguire tramite questo profilo di scansione.

12.2.3 Personalizzazione proprietà controlli di vulnerabilità

Tutti i controlli elencati nella scheda **Vulnerabilità** sono dotati di proprietà specifiche che determinano le modalità di attivazione del controllo e i dettagli enumerati durante una scansione.



Screenshot 130: Finestra di dialogo Proprietà vulnerabilità: scheda Generale

Per modificare le proprietà di un controllo di vulnerabilità:

1. Fare clic con il tasto destro del mouse sulla vulnerabilità da personalizzare e selezionare **Proprietà**.

2. Personalizzare il controllo di vulnerabilità selezionato dalle schede descritte di seguito:

Table 78: Finestra di dialogo Proprietà vulnerabilità

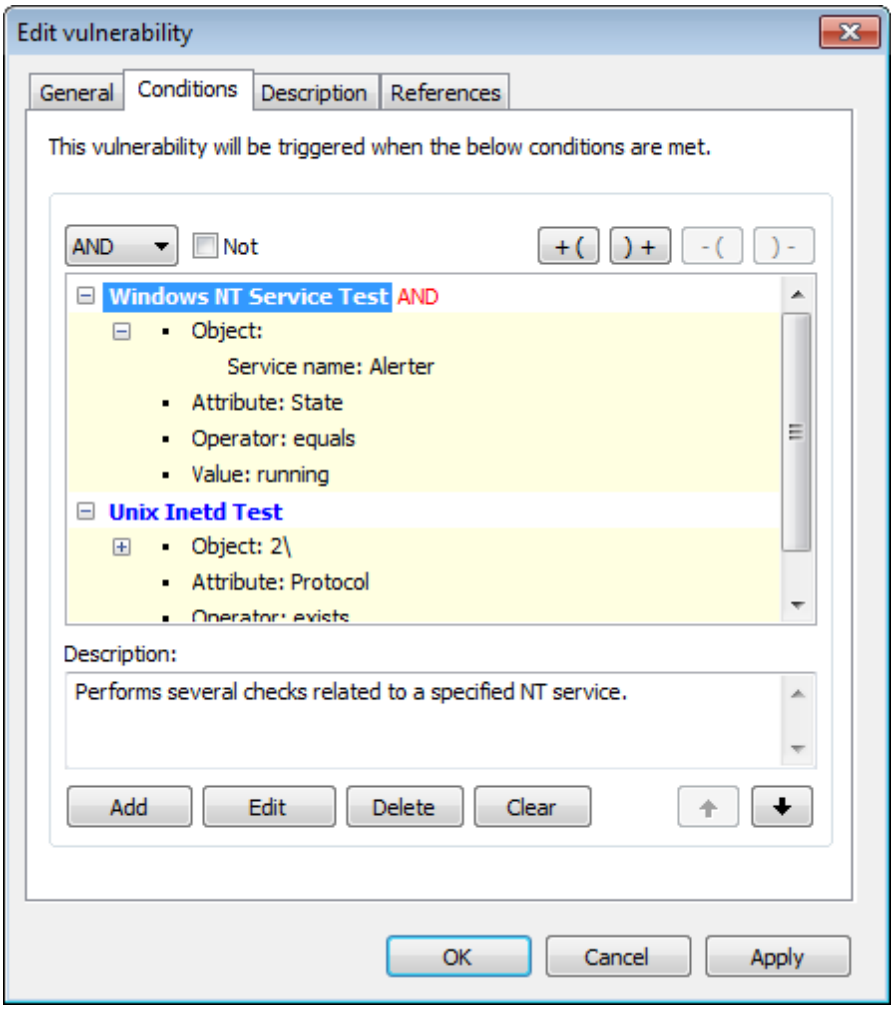
Scheda	Descrizione
Generale	Usare questa scheda per personalizzare i dettagli generali di un controllo di vulnerabilità, compresi il nome del controllo di vulnerabilità, il tipo di vulnerabilità, la famiglia del sistema operativo, la versione del sistema operativo, il prodotto, il formato temporale e la gravità.
Condizioni	Usare questa scheda per configurare i parametri operativi di questo controllo di vulnerabilità. Questi parametri definiranno se un controllo di vulnerabilità sia avvenuto o meno correttamente.
Descrizione	Usare questa scheda per personalizzare la descrizione del controllo di vulnerabilità.
Riferimenti	Usare questa scheda per personalizzare i riferimenti e i collegamenti alle informazioni rilevanti nei rapporti OVAL, CVE, MS Security, Security Focus e TOP 20 del SANS.

3. Fare clic su **OK** per salvare le impostazioni in uso.

12.2.4 Configurazione delle condizioni dei controlli di vulnerabilità

La scheda **Condizioni** consente di aggiungere o personalizzare le condizioni che definiscono la vulnerabilità o meno del/i computer o della/e rete/i sottoposti a scansione. È pertanto di

fondamentale importanza che i controlli personalizzati definiti in questa sezione vengano configurati da tecnici qualificati consapevoli delle ramificazioni delle proprie azioni.

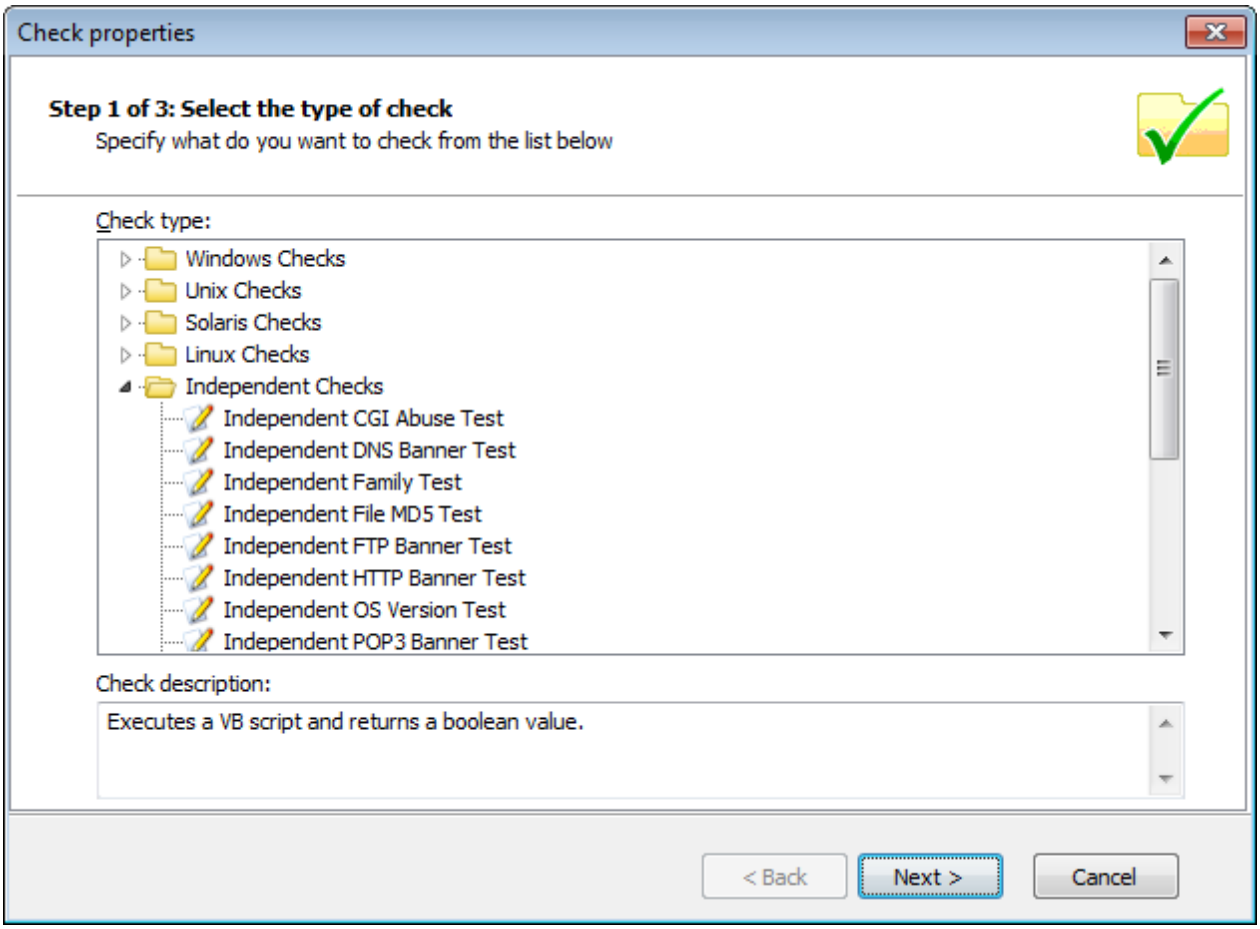


Screenshot 131: Scheda di configurazione delle condizioni di vulnerabilità

Per aggiungere una condizione di controllo di vulnerabilità:

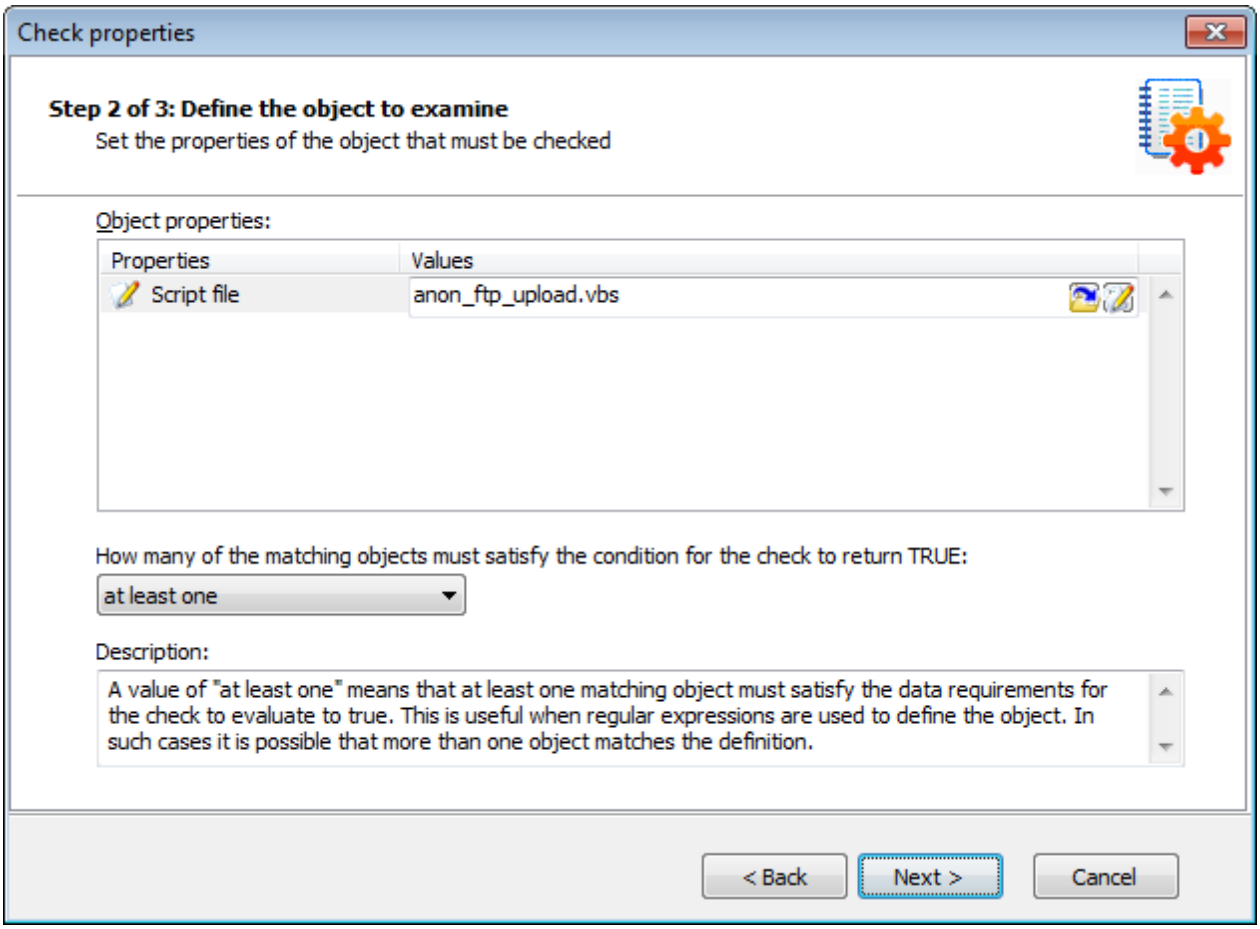
1. Dalla scheda **Opzioni di valutazione delle vulnerabilità** > sottoscheda **Vulnerabilità** fare clic con il pulsante destro del mouse su una vulnerabilità dall'elenco relativo, quindi selezionare **Proprietà**.

2. Dalla finestra di dialogo **Modifica vulnerabilità** fare clic sulla scheda **Condizioni>Aggiungi**.



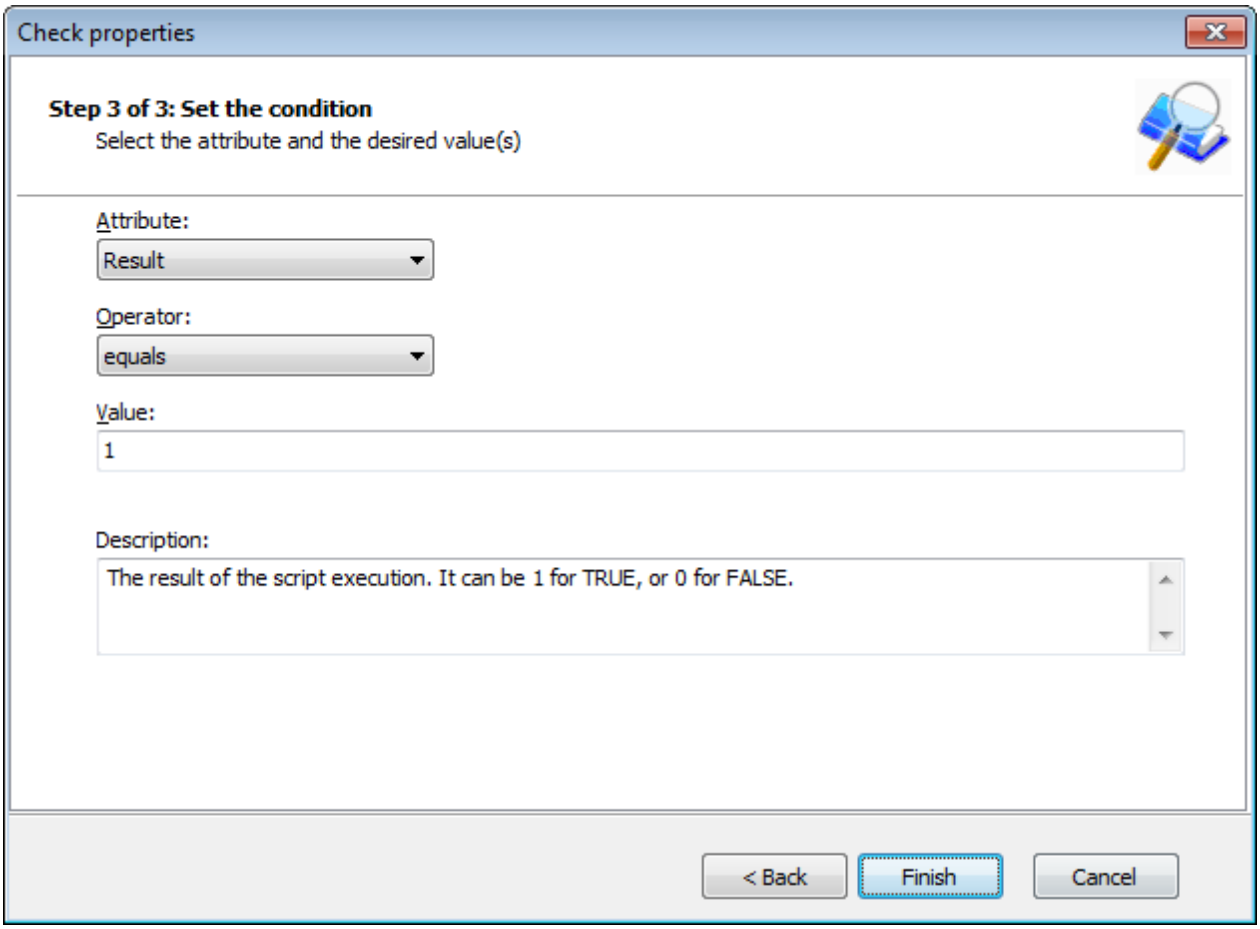
Screenshot 132: Procedura guidata Proprietà controllo - Selezione del tipo di controllo

3. Selezionare il tipo di controllo da configurare e fare clic su **Avanti**.


Check properties
Step 2 of 3: Define the object to examine
Set the properties of the object that must be checked
Object properties:
Properties
Values
Script file
anon_ftp_upload.vbs
How many of the matching objects must satisfy the condition for the check to return TRUE:
at least one
Description:
A value of "at least one" means that at least one matching object must satisfy the data requirements for the check to evaluate to true. This is useful when regular expressions are used to define the object. In such cases it is possible that more than one object matches the definition.
< Back
Next >
Cancel

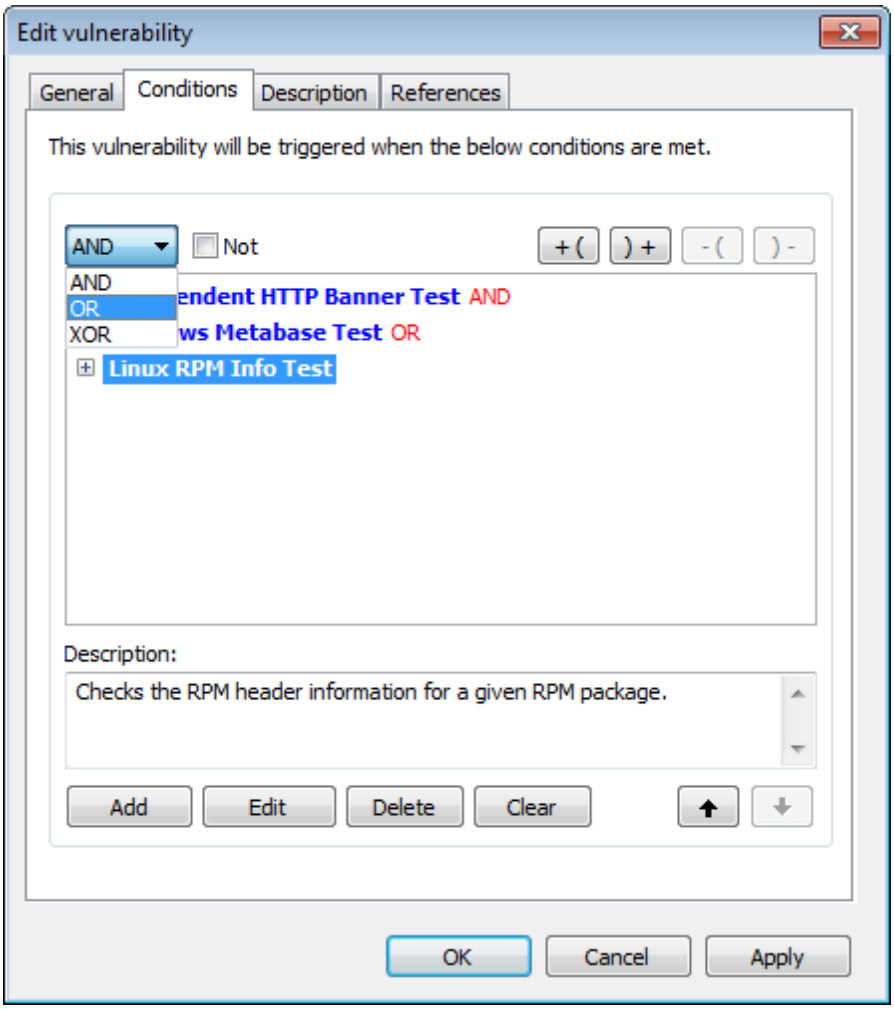
Screenshot 133: Procedura guidata Proprietà controllo - Definizione dell'oggetto da esaminare

4. Definire l'oggetto da esaminare e fare clic su **Avanti**.



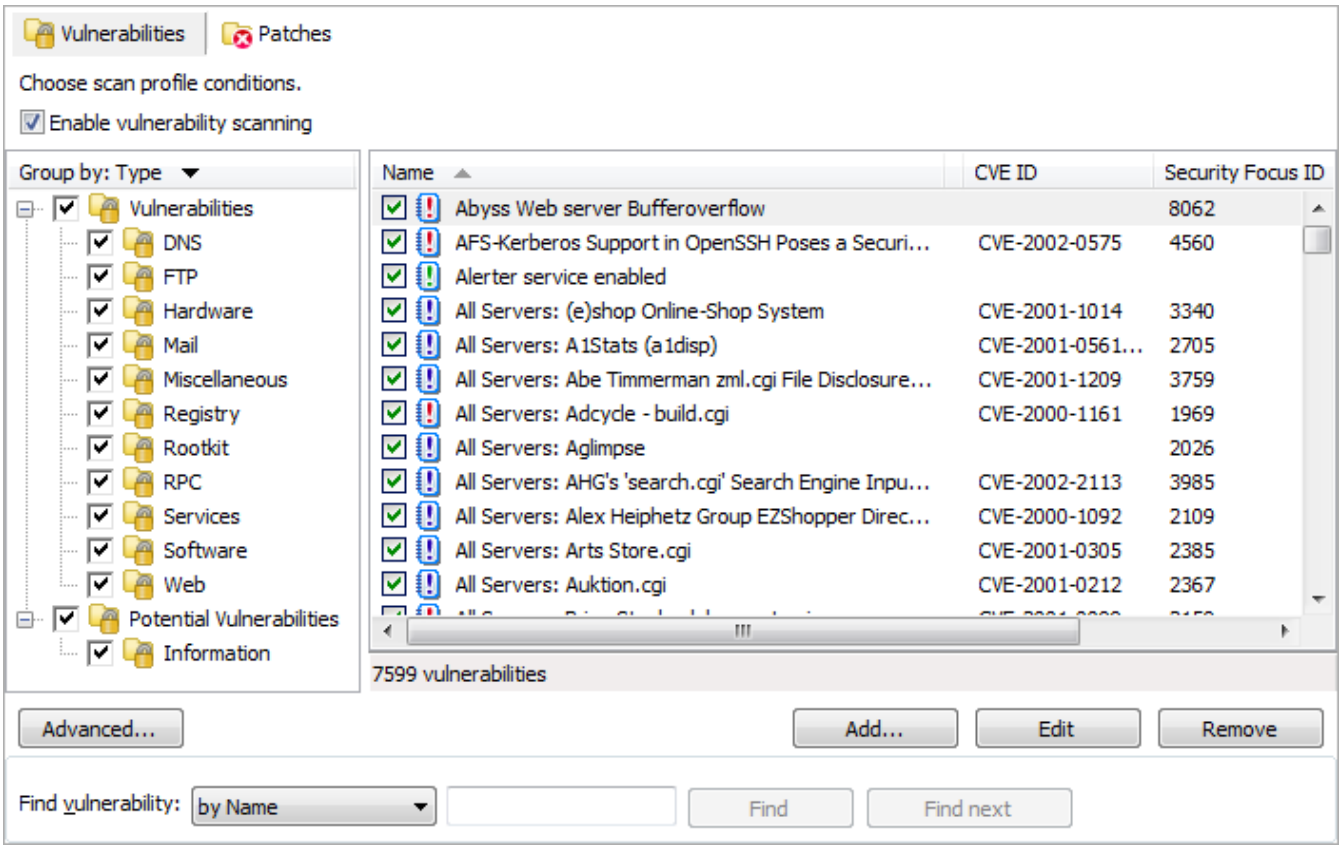
Screenshot 134: Procedura guidata Proprietà controllo - Impostazione delle condizioni necessarie

5. Specificare le condizioni necessarie e fare clic su **Fine** per finalizzare le impostazioni.



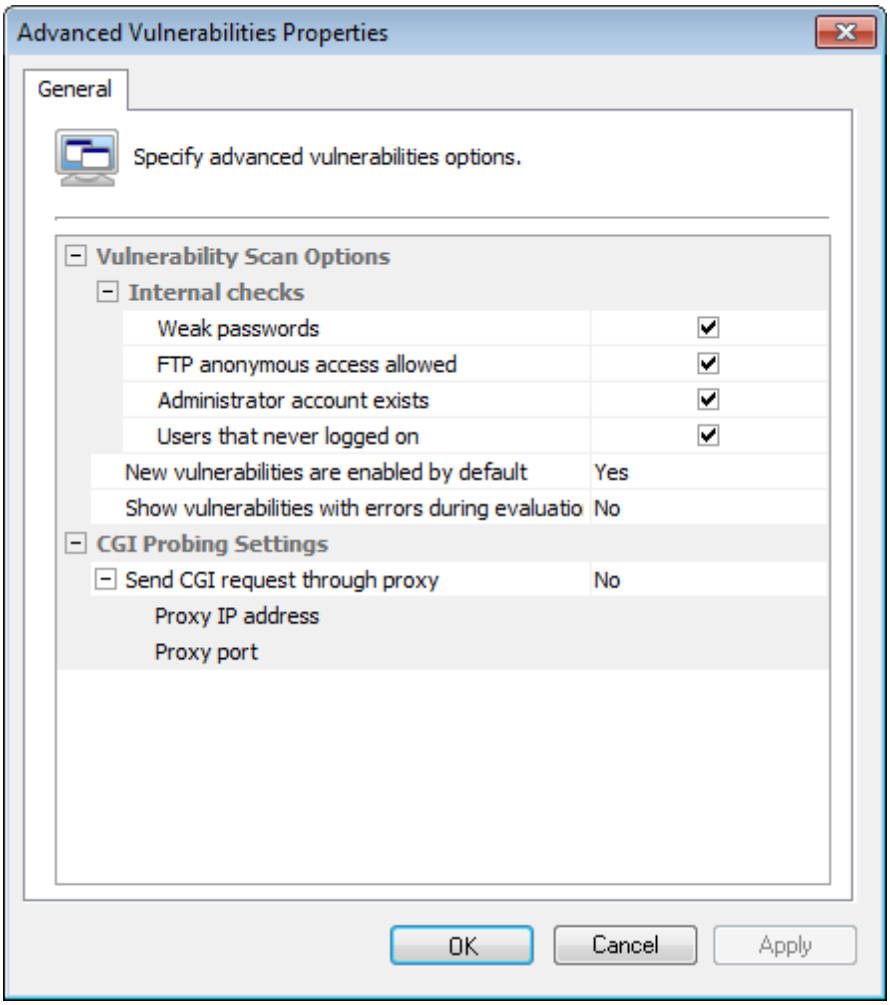
Screenshot 135: Procedura guidata Proprietà controllo - Definizione degli operatori condizionali

6. Se è stata configurata più di una condizione, definire gli operatori condizionali e fare clic su **OK** per completare le impostazioni di configurazione.



Screenshot 136: Opzioni avanzate di vulnerabilità

7. (Facoltativo) Dalla scheda **Vulnerabilità**, fare clic su **Avanzate** per richiamare le opzioni di scansione delle vulnerabilità avanzate.



Screenshot 137: Finestre di dialogo Scansione delle vulnerabilità avanzate

Opzioni vulnerabilità avanzate sono utilizzate per:

- Configurare le funzioni estese di scansione delle vulnerabilità che ricercano sui computer di destinazione password deboli, accessi FTP anonimi o account utenti inutilizzati.
- Configurare il modo in cui GFI LanGuard gestirà i controlli di vulnerabilità appena creati.
- Configurare GFI LanGuard affinché invii delle richieste CGI attraverso uno specifico server proxy. Questa impostazione è obbligatoria quando le richieste CGI vengono inviate da un computer protetto da un firewall a un server Web di destinazione "al di fuori" del firewall, ad esempio, i server Web in una DMZ.

Il firewall solitamente bloccherà tutte le richieste CGI inviate direttamente da GFI LanGuard a un computer di destinazione che si trova davanti al firewall. Per evitare che ciò avvenga, impostare su 'Sì' l'opzione **Invia richieste CGI tramite proxy** e specificare il nome/l'indirizzo IP del server proxy e la porta di comunicazione utilizzati per inviare la richiesta CGI alla destinazione.

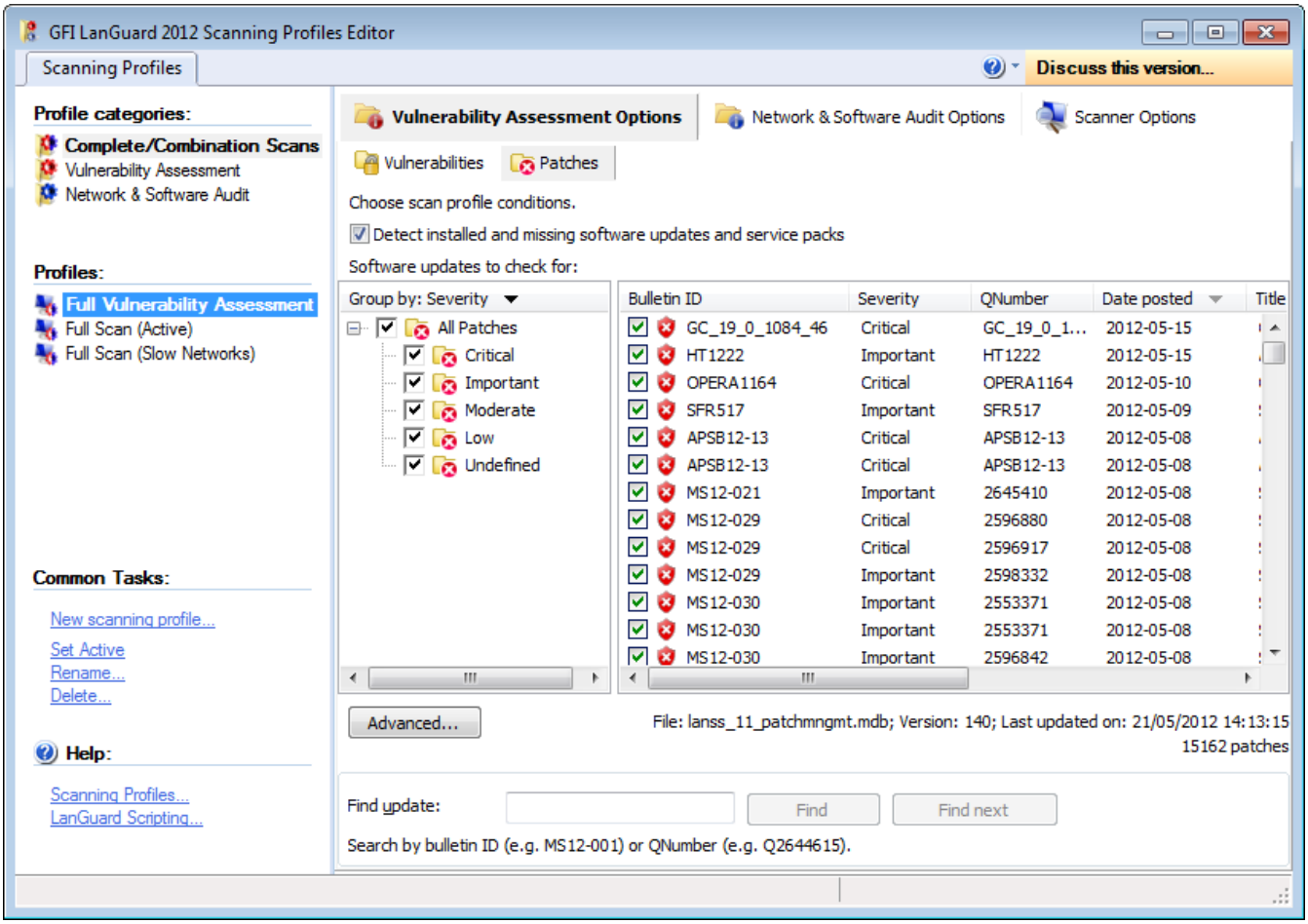
12.3 Configurazione delle patch

La scheda **Patch** specifica gli aggiornamenti di sicurezza da ricercare durante la scansione delle vulnerabilità. Le patch controllate vengono selezionate da un elenco completo di aggiornamenti software supportati che sono inclusi in questa scheda. Questo elenco viene automaticamente aggiornato ogni volta che GFI rilascia un nuovo aggiornamento di un file di definizione di una patch mancante per GFI LanGuard.

Le seguenti sezioni contengono informazioni relative a:

- Abilitazione/Disabilitazione dei controlli di rilevamento delle patch mancanti
- Personalizzazione dell'elenco delle patch software da sottoporre a scansione
- Ricerca di informazioni in un bollettino

12.3.1 Abilitazione/Disabilitazione dei controlli di rilevamento delle patch mancanti



Screenshot 138: Proprietà Profili di scansione: opzioni scheda Patch

Per abilitare il rilevamento delle patch mancanti in un particolare profilo di scansione:

1. Avviare GFI LanGuard.

2. Fare clic sul pulsante GFI LanGuard e selezionare **Configurazione > Editor dei profili di scansione**. In alternativa, premere **CTRL + P** per avviare l'**Editor profili di scansione**.

3. Nella scheda **Opzioni di valutazione delle vulnerabilità** fare clic sulla sottoscheda **Patch**.

4. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**.

5. Nel riquadro di destra selezionare l'opzione **Rileva service pack/patch installati e mancanti**.

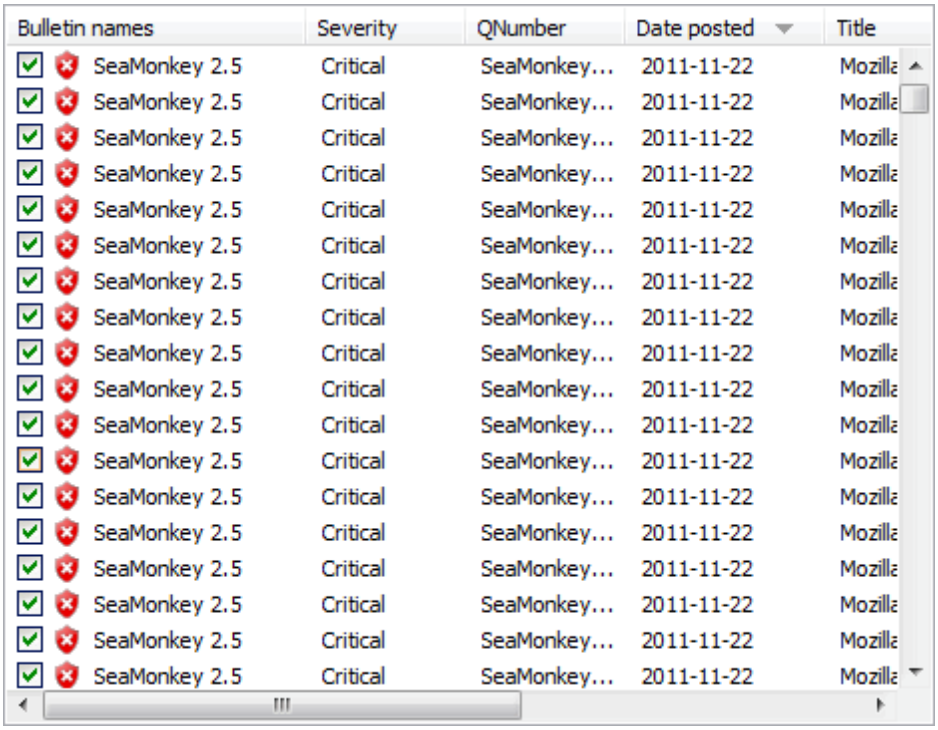
> **Nota**
>
> I parametri di scansione delle patch mancanti possono essere configurati in un profilo di scansione specifico per quel profilo. Assicurarsi di abilitare le patch mancanti in tutti i profili all'interno dei quali è necessario eseguire una scansione delle patch mancanti.

12.3.2 Personalizzazione dell'elenco delle patch software da sottoporre a scansione

Per specificare gli aggiornamenti di sicurezza mancanti da enumerare ed elaborare all'interno di un profilo di scansione:

1. Nella scheda **Opzioni di valutazione delle vulnerabilità**, fare clic sulla sottoscheda **Patch**.

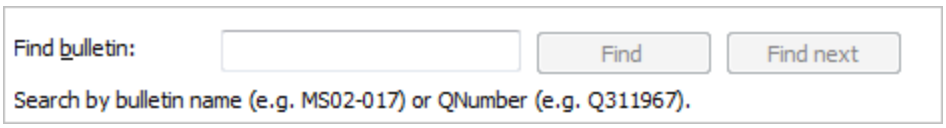
2. Selezionare il profilo di scansione da personalizzare dal riquadro di sinistra sotto **Profili**.



Screenshot 139: Selezionare le patch mancanti da enumerare

3. Nel riquadro di destra, selezionare/deselezionare le patch mancanti da enumerare all'interno di questo profilo di scansione.

12.3.3 Ricerca di informazioni in un bollettino

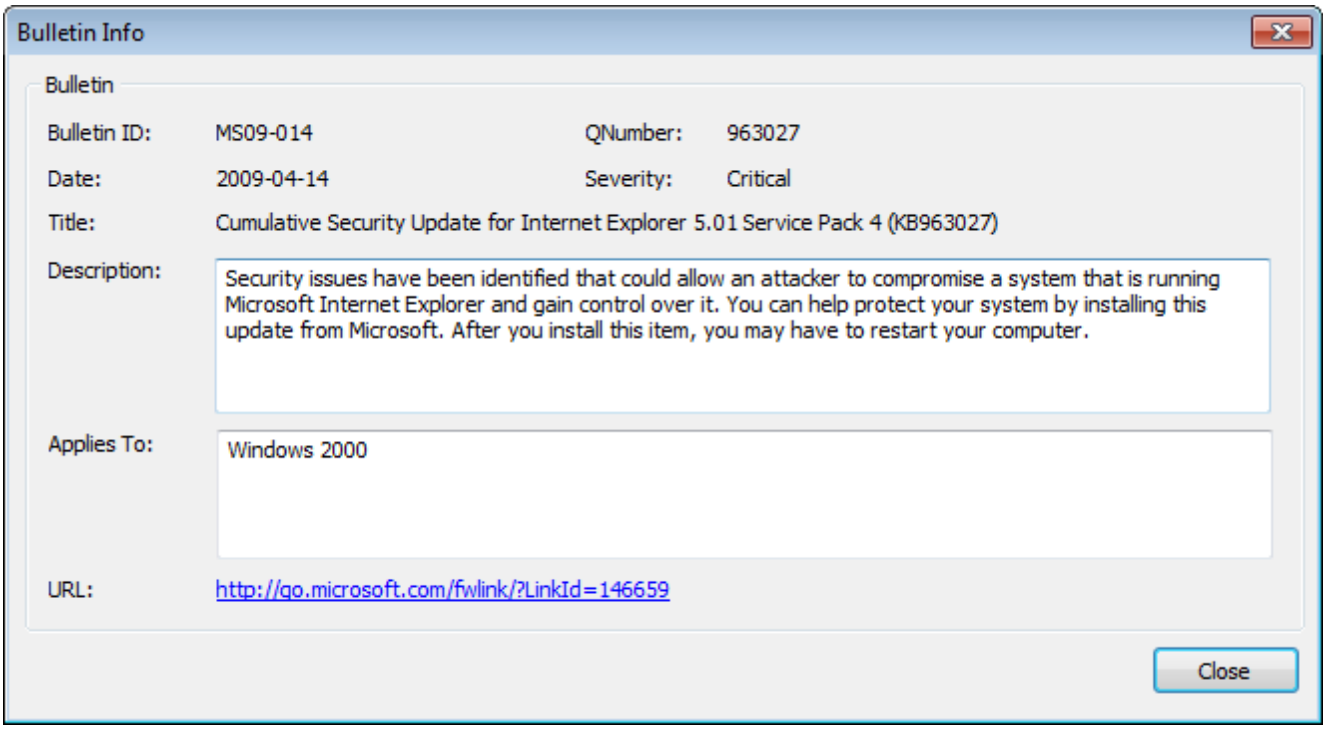


Screenshot 140: Ricerca di informazioni in un bollettino

Per cercare uno specifico bollettino:

1. Da **Opzioni di valutazione delle vulnerabilità > Vulnerabilità > Trova bollettino** specificare il nome del bollettino (esempio: MS02-017) o QNumber (esempio: Q311987) nella casella dello strumento di ricerca nella parte inferiore del riquadro di destra.

2. Fare clic su **Trova** per cercare la voce.


Bulletin Info
Bulletin
Bulletin ID:
MS09-014
QNumber:
963027
Date:
2009-04-14
Severity:
Critical
Title:
Cumulative Security Update for Internet Explorer 5.01 Service Pack 4 (KB963027)
Description:
Security issues have been identified that could allow an attacker to compromise a system that is running Microsoft Internet Explorer and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this item, you may have to restart your computer.
Applies To:
Windows 2000
URL:
http://go.microsoft.com/fwlink/?LinkId=146659
Close

Screenshot 141: Informazioni estese del bollettino

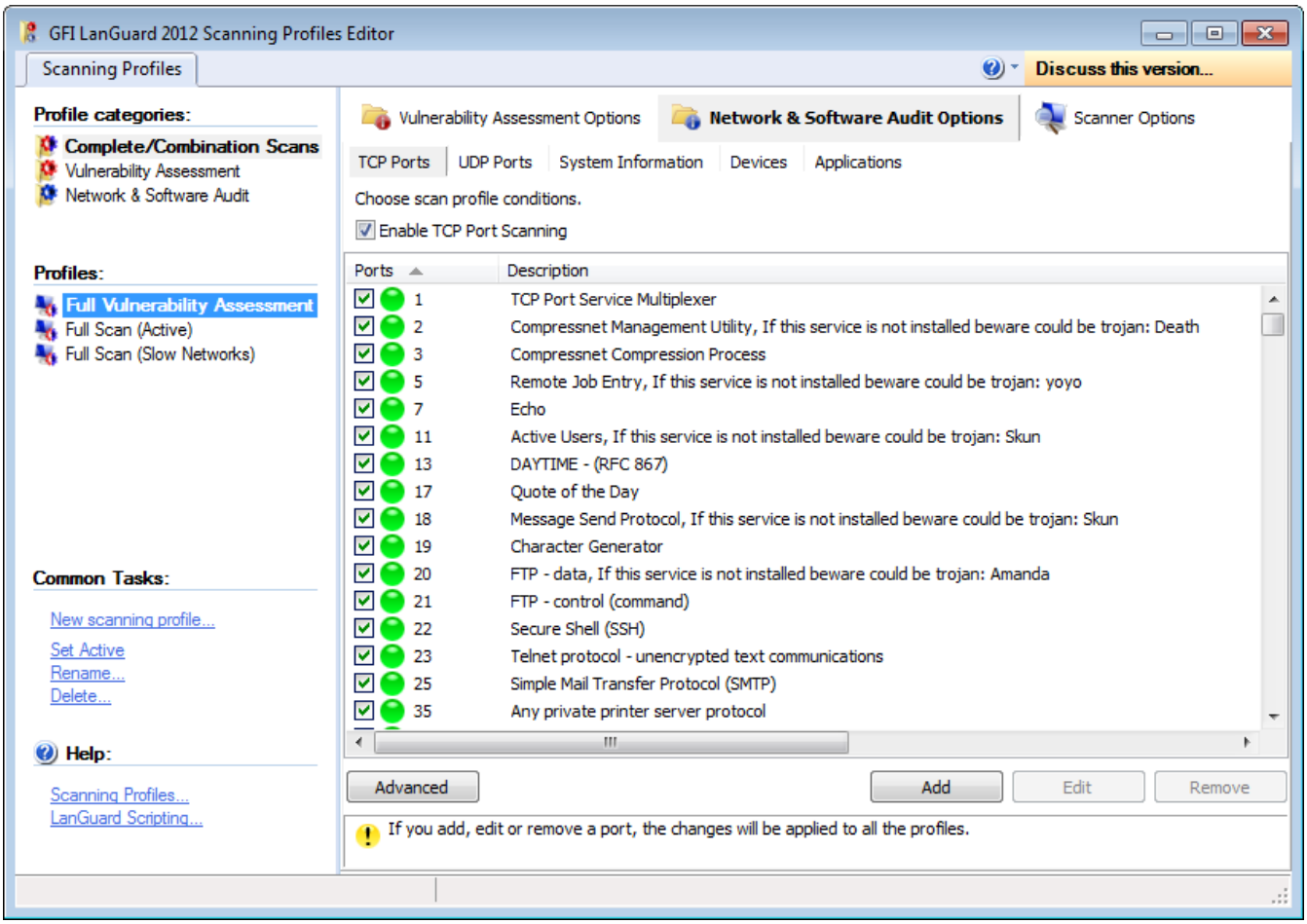
12.4 Configurazione opzioni di controllo rete e software

I profili di scansione forniti con GFI LanGuard sono stati preconfigurati per l'esecuzione di una serie di controlli di rete e software sulla destinazione selezionata. È possibile tuttavia disabilitare la scansione e personalizzare l'elenco dei controlli di rete e di software eseguiti durante una scansione.

Questa sezione contiene informazioni relative a:

- Configurazione opzioni di scansione per la porta TCP/UDP
- Configurazione opzioni Informazioni di sistema
- Configurazione opzioni di scansione dei dispositivi
- Configurazione delle opzioni di scansione delle applicazioni

12.4.1 Configurazione opzioni di scansione per la porta TCP/UDP


GFI LanGuard 2012 Scanning Profiles Editor
Scanning Profiles
Discuss this version...
Profile categories:
Complete/Combination Scans
Vulnerability Assessment
Network & Software Audit
Profiles:
Full Vulnerability Assessment
Full Scan (Active)
Full Scan (Slow Networks)
Common Tasks:
New scanning profile...
Set Active
Rename...
Delete...
Help:
Scanning Profiles...
LanGuard Scripting...
Vulnerability Assessment Options
Network & Software Audit Options
Scanner Options
TCP Ports
UDP Ports
System Information
Devices
Applications
Choose scan profile conditions.
Enable TCP Port Scanning
Ports
Description
1 TCP Port Service Multiplexer
2 Compressnet Management Utility, If this service is not installed beware could be trojan: Death
3 Compressnet Compression Process
5 Remote Job Entry, If this service is not installed beware could be trojan: yoyo
7 Echo
11 Active Users, If this service is not installed beware could be trojan: Skun
13 DAYTIME - (RFC 867)
17 Quote of the Day
18 Message Send Protocol, If this service is not installed beware could be trojan: Skun
19 Character Generator
20 FTP - data, If this service is not installed beware could be trojan: Amanda
21 FTP - control (command)
22 Secure Shell (SSH)
23 Telnet protocol - unencrypted text communications
25 Simple Mail Transfer Protocol (SMTP)
35 Any private printer server protocol
Advanced
Add
Edit
Remove
If you add, edit or remove a port, the changes will be applied to all the profiles.

Screenshot 142: Proprietà Profili di scansione: opzioni scheda Porte TCP

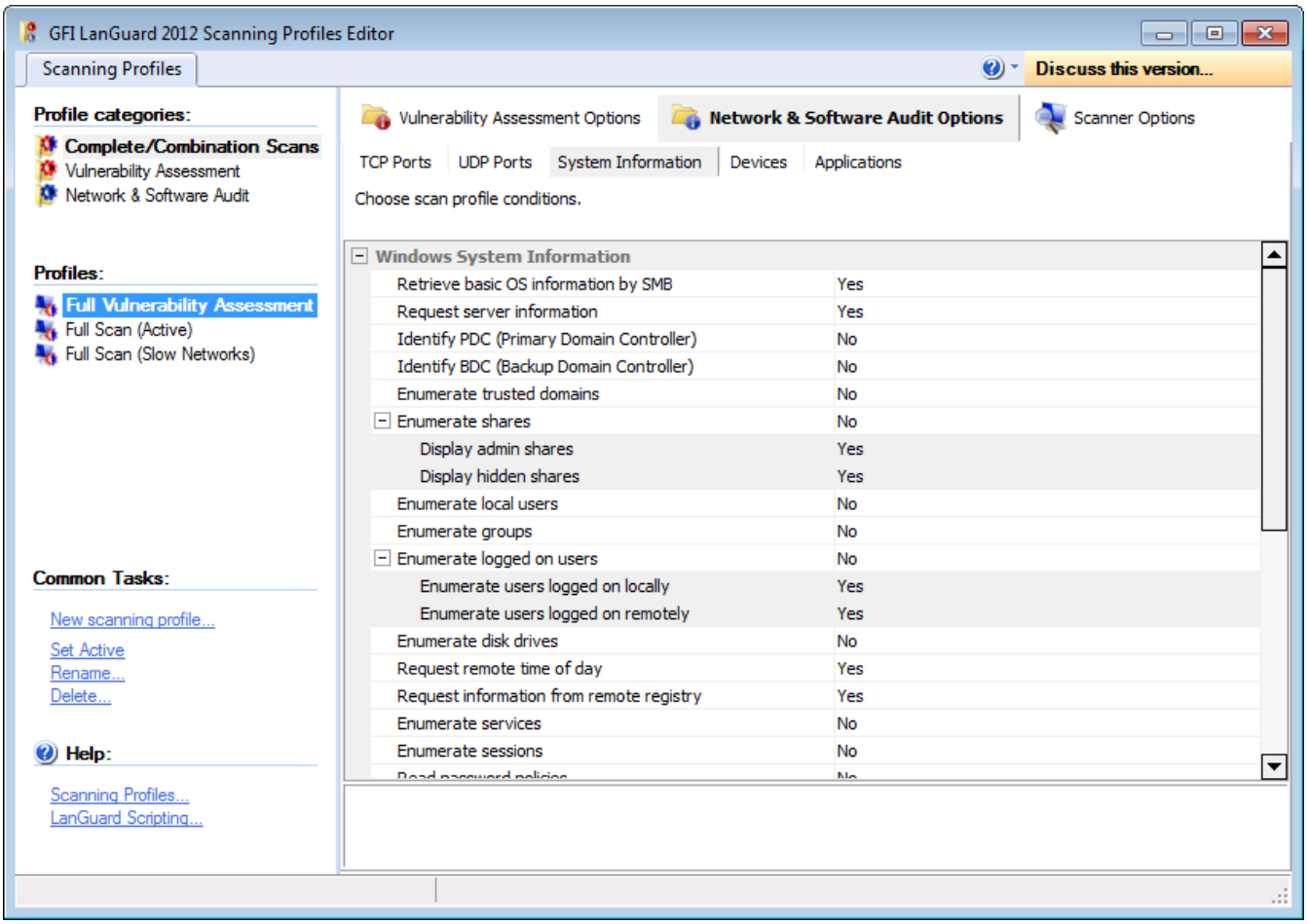
Table 79: Opzioni di scansione della porta TCP

Opzione	Descrizione
Abilitazione/Disabilitazione della scansione sulle porte TCP	Per abilitare la scansione delle porte TCP in un particolare profilo di scansione: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Porte TCP**. 2. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**. 3. Selezionare l'opzione **Abilita scansione delle porte TCP**.
Configurazione dell'elenco delle porte TCP da sottoporre a scansione	Per configurare quali porte TCP verranno elaborate da un profilo di scansione: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Porte TCP**. 2. Selezionare il profilo di scansione da personalizzare dal riquadro di sinistra sotto **Profili**. 3. Selezionare le porte TCP da analizzare con questo profilo di scansione.
Personalizzazione dell'elenco di porte TCP	1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Porte TCP**. 2. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**. 3. Personalizzare l'elenco delle porte TCP utilizzando le funzioni **Aggiungi**, **Modifica** o **Rimuovi**.

Nota

L'elenco di porte TCP/UDP è comune a tutti i profili. L'eliminazione di una porta dall'elenco la renderà non disponibile per tutti i profili di scansione.

12.4.2 Configurazione opzioni Informazioni di sistema



Screenshot 143: Proprietà Profili di scansione: opzioni della scheda Informazioni di sistema

Per specificare le **Informazioni di sistema** enumerate da un particolare profilo di scansione:

1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Informazioni di sistema**.

2. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**.

3. Dal riquadro di destra, espandere il gruppo **Informazioni di sistema di Windows** o Informazioni di sistema di Linux in base alla necessità.

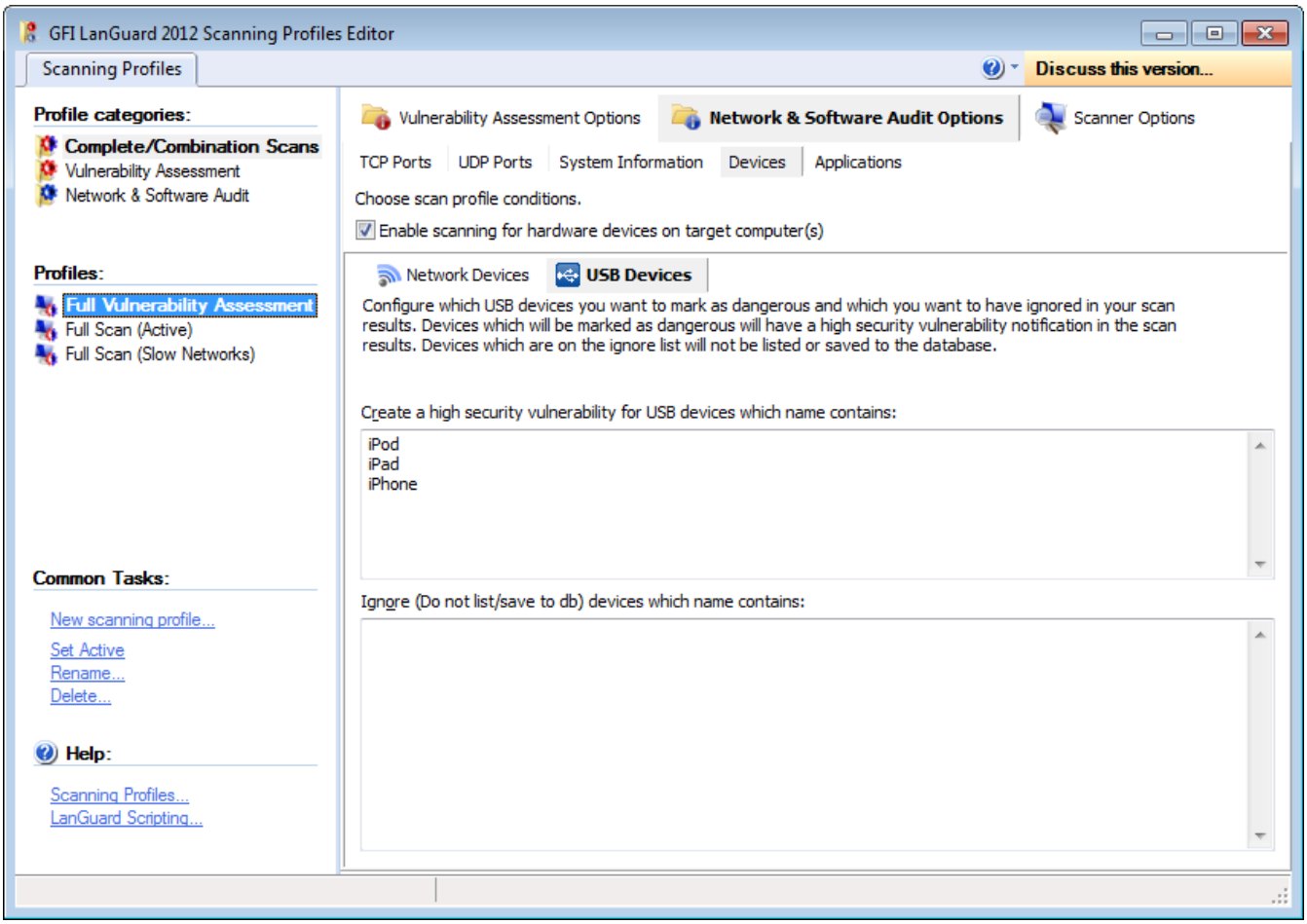
4. Selezionare le informazioni del sistema operativo Windows/Linux che lo scanner di sicurezza deve recuperare dalle destinazioni sottoposte a scansione.

Ad esempio, per enumerare le condivisioni amministrative e i risultati della scansione, espandere l'opzione **Enumera condivisioni** e impostare l'opzione **Visualizza condivisioni amministrative** su **'Sì'**.

12.4.3 Configurazione opzioni di scansione dei dispositivi

Usare la scheda Dispositivi per enumerare i dispositivi di rete. Insieme all'enumerazione dei dispositivi, è possibile configurare GFI LanGuard in modo da ricevere un avviso in caso di vulnerabilità di sicurezza di livello alto ogni volta che viene rilevata una periferica USB o di rete.

Ciò è possibile compilando un elenco di reti e periferiche USB non autorizzate/inserite in una lista nera per le quali si desidera ricevere una notifica.


GFI LanGuard 2012 Scanning Profiles Editor
Scanning Profiles
Discuss this version...
Profile categories:
Complete/Combination Scans
Vulnerability Assessment
Network & Software Audit
Profiles:
Full Vulnerability Assessment
Full Scan (Active)
Full Scan (Slow Networks)
Common Tasks:
New scanning profile...
Set Active
Rename...
Delete...
Help:
Scanning Profiles...
LanGuard Scripting...
Vulnerability Assessment Options
Network & Software Audit Options
Scanner Options
TCP Ports
UDP Ports
System Information
Devices
Applications
Choose scan profile conditions.
Enable scanning for hardware devices on target computer(s)
Network Devices
USB Devices
Configure which USB devices you want to mark as dangerous and which you want to have ignored in your scan results. Devices which will be marked as dangerous will have a high security vulnerability notification in the scan results. Devices which are on the ignore list will not be listed or saved to the database.
Create a high security vulnerability for USB devices which name contains:
iPod
iPad
iPhone
Ignore (Do not list/save to db) devices which name contains:

Screenshot 144: Pagina di configurazione dei dispositivi di rete

GFI LanGuard può anche escludere dal processo di scansione periferiche USB specifiche considerate “sicure”, quali mouse USB o tastiere. Ciò è possibile mediante una whitelist/lista sicura di periferiche USB che dovranno essere ignorate durante le scansioni.

In modo simile, è possibile creare un profilo di scansione separato che enumera solo i dongle Bluetooth e le schede NIC wireless collegate ai computer di destinazione in uso. In questo caso, tuttavia, è necessario specificare "Bluetooth" e "Wireless” o “WiFi” negli elenchi delle reti e delle periferiche USB non autorizzate del profilo di scansione.

È possibile accedere a tutte le opzioni di configurazione della scansione dei dispositivi tramite le due sottoschede contenute nella pagina di configurazione dei dispositivi. Queste sottoschede si chiamano **Dispositivi di rete** e **Periferiche USB**.

Utilizzare la sottoscheda **Dispositivi di rete** per configurare le opzioni di scansione dei dispositivi di rete collegati e gli elenchi dei dispositivi della blacklist (non autorizzati)/whitelist (sicuri).

Utilizzare la sottoscheda **Periferiche USB** per configurare le opzioni di scansione delle periferiche USB collegate e gli elenchi dei dispositivi non autorizzati/sicuri.

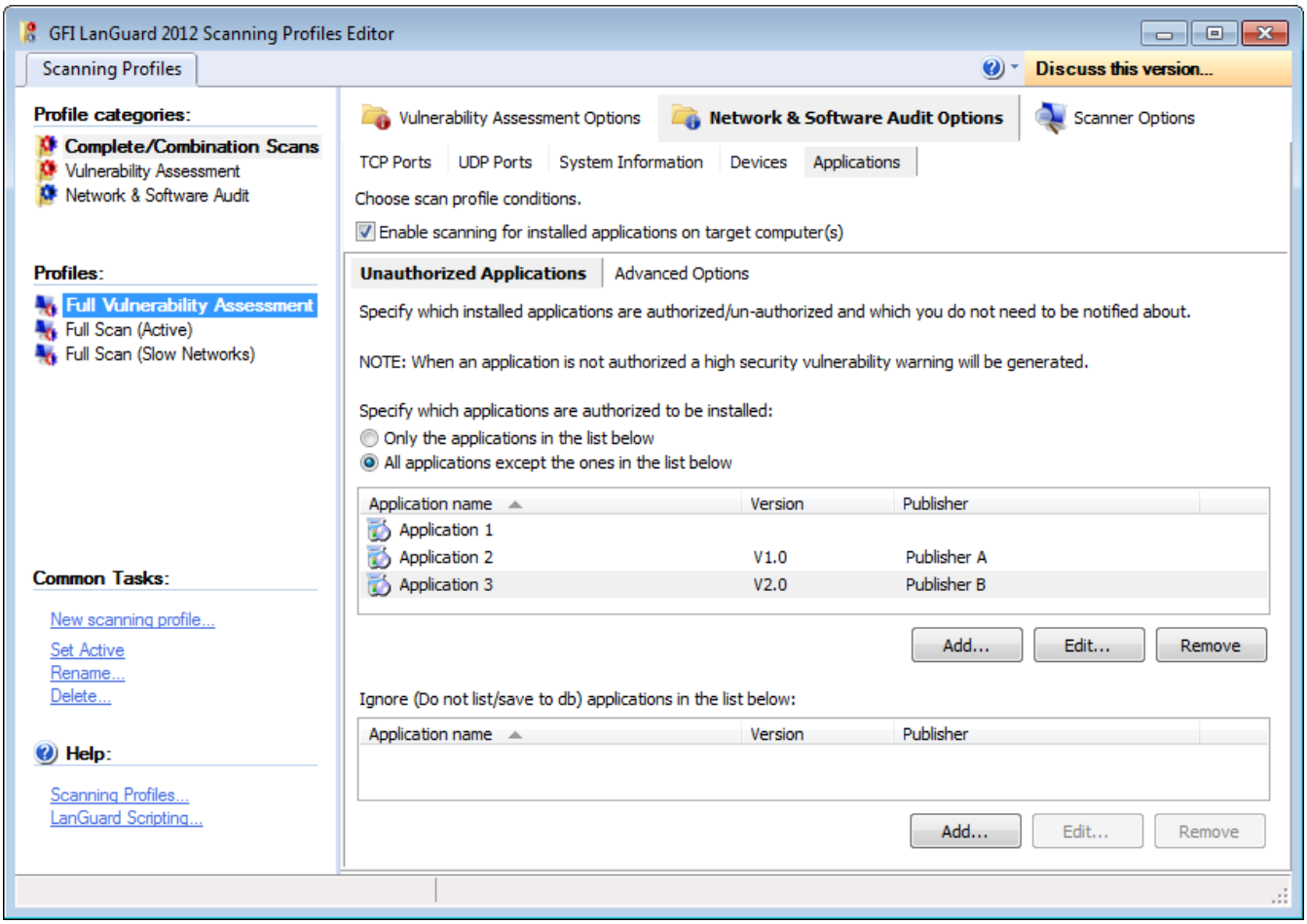
Table 80: Opzioni di scansione del dispositivo

Opzione	Descrizione
Abilitazione/Disabilitazione dei controlli per tutti i dispositivi di rete installati	Per abilitare la scansione dei dispositivi di rete (incluse le periferiche USB) in un particolare profilo di scansione: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Dispositivi**. 2. Fare clic sulla scheda **Dispositivi di rete**. 3. Selezionare il profilo di scansione da personalizzare dal riquadro di sinistra sotto **Profili**. 4. Dal riquadro di destra, selezionare **Abilita la scansione dei dispositivi hardware** sul/i computer di destinazione. **Nota** La scansione dei dispositivi di rete può essere configurata in base a un profilo di scansione specifico. Assicurarsi di abilitare la scansione dei dispositivi in tutti i profili all'interno dei quali è necessaria.
Compilazione di una blacklist/whitelist dei dispositivi di rete	Per compilare una blacklist/whitelist dei dispositivi di rete per un profilo di scansione: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Dispositivi**. 2. Fare clic sulla scheda **Dispositivi di rete**. 3. Selezionare il profilo di scansione da personalizzare dal riquadro di sinistra sotto **Profili**. 4. Nel riquadro di destra: per creare una blacklist dei dispositivi di rete, specificare i dispositivi da classificare come vulnerabilità di sicurezza di livello alto nello spazio a disposizione sotto **Crea una vulnerabilità di sicurezza di livello alto per i dispositivi di rete il cui nome contiene**. Ad esempio, se si inserisce la parola "wireless", si riceverà una notifica per mezzo di un avviso di vulnerabilità di livello alto ogni volta che viene rilevato un dispositivo il cui nome contiene la parola "wireless". Per creare una whitelist di dispositivi, specificare i dispositivi da ignorare durante la scansione delle vulnerabilità di rete nello spazio a disposizione sotto **Ignora (non elencare/salva nel db)** i dispositivi il cui nome contiene. **Nota** Includere un solo nome di dispositivo di rete per riga.
Configurazione delle opzioni di scansione avanzate di un dispositivo di rete	Dalla scheda **Dispositivi di rete**, è anche possibile specificare il tipo di dispositivo di rete controllato dal profilo di scansione e registrato nei risultati della scansione. Tali funzioni comprendono: dispositivi di rete cablati, dispositivi di rete wireless, dispositivi di rete enumerati dal software e dispositivi di rete virtuali. Per specificare i dispositivi di rete da enumerare nei risultati della scansione: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Dispositivi**. 2. Fare clic sulla scheda **Dispositivi di rete** (si apre per impostazione predefinita). 3. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**. 4. Fare clic su **Avanzate** nella parte inferiore della pagina. 5. Impostare le opzioni necessarie su **Sì**. Fare clic su **OK** per completare le impostazioni in uso.

Opzione	Descrizione
Scansione delle periferiche USB	Per compilare un elenco di periferiche USB non autorizzate/non sicure: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Dispositivi**. 2. Fare clic sulla scheda **Periferiche USB**. 3. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**. 4. Nel riquadro di destra specificare i dispositivi da classificare come vulnerabilità di sicurezza di livello alto nello spazio a disposizione sotto **Crea una vulnerabilità di sicurezza di livello alto per le periferiche USB il cui nome contiene:**. Ad esempio, se si inserisce la parola "iPod", si riceverà una notifica per mezzo di un avviso di vulnerabilità di livello alto ogni volta che viene rilevato una periferica USB il cui nome contiene la parola "iPod". Per creare una whitelist di periferiche USB, specificare le periferiche USB da ignorare durante la scansione delle vulnerabilità di rete nello spazio a disposizione sotto **Ignora (non elencare/salva nel db) i dispositivi il cui nome contiene**. **Nota** Includere un solo nome di periferica USB per riga.

12.4.4 Configurazione delle opzioni di scansione delle applicazioni

La scheda **Applicazioni** consente di specificare le applicazioni che attiveranno un avviso durante una scansione.



Screenshot 145: Pagina di configurazione delle applicazioni

All'interno di questa scheda, è possibile configurare GFI LanGuard in modo da rilevare il software non autorizzato installato sulle destinazioni sottoposte a scansione e generare un avviso di vulnerabilità di sicurezza di livello alto ogni volta che viene rilevato un software di questo tipo.

Table 81: Opzioni di scansione delle applicazioni

Opzione	Descrizione
Scansione delle applicazioni installate	Per impostazione predefinita, GFI LanGuard supporta anche l'integrazione con particolari applicazioni di sicurezza. Queste applicazioni comprendono vari software antivirus e antispyware. Durante la scansione di sicurezza, GFI LanGuard verifica che il software antispyware o di scansione dei virus sia configurato correttamente e che i rispettivi file di definizione siano aggiornati. La scansione delle applicazioni può essere configurata a livello di profilo di scansione in modo specifico per ciascun profilo ed è possibile accedere a tutte le opzioni di configurazione tramite le due sottoschede contenute nella scheda **Applicazioni**. Queste sottoschede si chiamano **Applicazioni non autorizzate** e **Opzioni avanzate**.

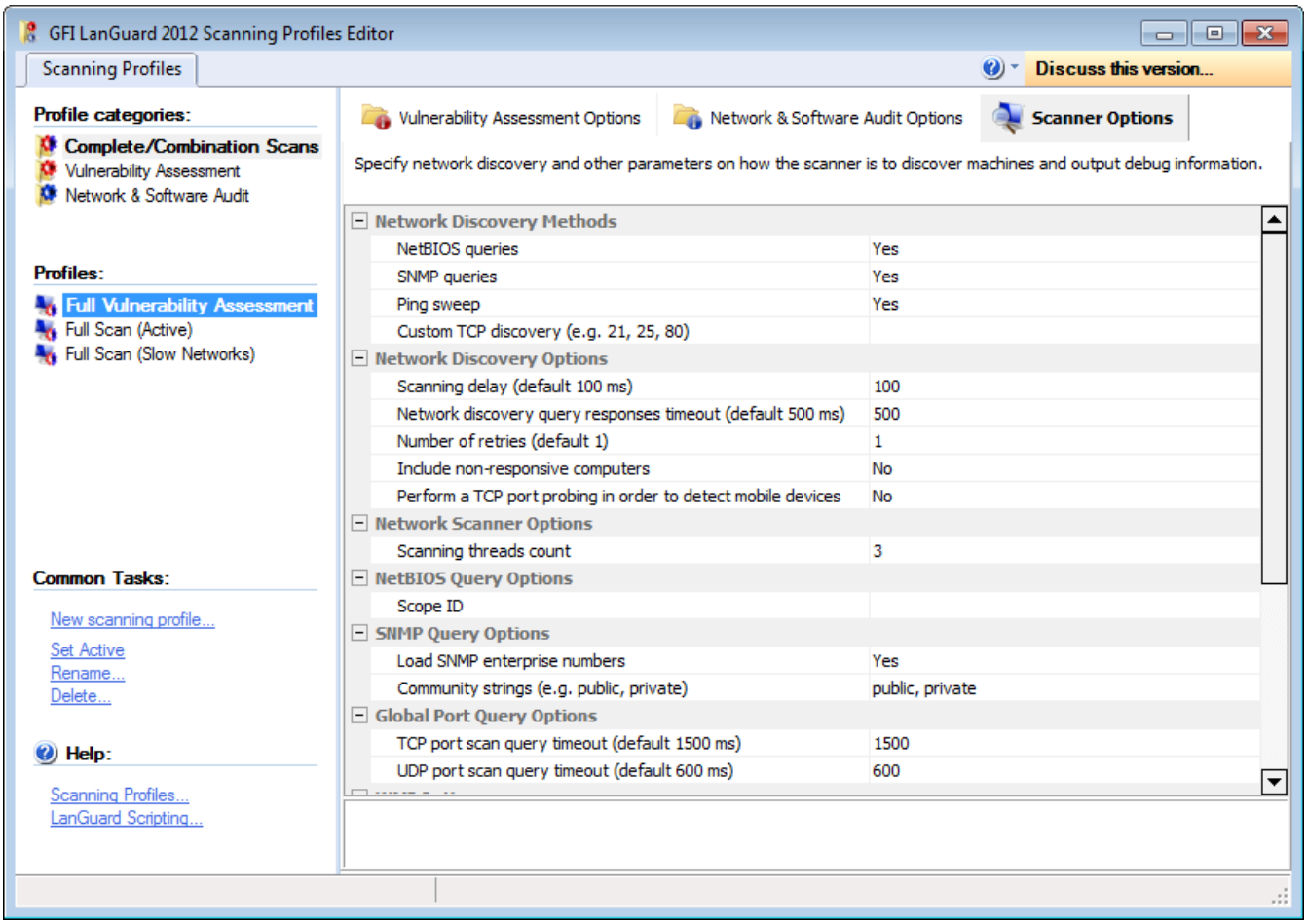
Opzione	Descrizione
Abilitazione/Disabilitazione dei controlli per le applicazioni installate	Per abilitare la scansione delle applicazioni installate in un particolare profilo di scansione: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Applicazioni**. 2. Fare clic sulla sottoscheda **Applicazioni non autorizzate**. 3. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**. 4. Selezionare la casella di controllo **Abilita scansione per le applicazioni installate sui computer di destinazione**. **Nota** La scansione delle applicazioni installate può essere configurata in un profilo di scansione in modo specifico per quel profilo. Assicurarsi di abilitare la scansione delle applicazioni installate in tutti i profili all'interno dei quali è necessaria.
Compilazione di una blacklist/whitelist delle applicazioni installate	Per compilare una blacklist/whitelist delle applicazioni installate: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Applicazioni**. 2. Selezionare la sottoscheda **Applicazioni non autorizzate**. 3. Selezionare il profilo di scansione da personalizzare dal riquadro di sinistra sotto **Profili**. 4. Dal riquadro a destra, selezionare la casella di controllo **Abilita scansione per le applicazioni installate sui computer di destinazione**. 5. Specificare le applicazioni che sono autorizzate per l'installazione. Scegliere una delle seguenti opzioni: » **Solo i computer indicati nell'elenco**: specificare i nomi delle applicazioni che sono autorizzate per l'installazione. Verranno ignorate durante la scansione di sicurezza. » **Tutte le applicazioni eccetto quelle nell'elenco di seguito**: specificare i nomi delle applicazioni che non sono autorizzate per l'installazione. Le applicazioni non presenti in questo elenco verranno ignorate durante una scansione di sicurezza. 6. Nelle opzioni **Ignora (non elencare/salva nel db) le applicazioni il cui nome contiene:**, digitare le applicazioni facendo clic su **Aggiungi**. Qualsiasi applicazione elencata viene inserita nella whitelist. **Nota** Includere solo un nome di applicazione per riga.

Opzione	Descrizione
Opzioni avanzate di scansione delle applicazioni	GFI LanGuard viene fornito con un elenco predefinito di applicazioni antivirus e antispyware che possono essere controllate durante la scansione di sicurezza. La scheda **Opzioni avanzate** consente di configurare in GFI LanGuard la generazione di avvisi per le vulnerabilità a rischio alto, qualora rilevi determinate configurazioni di un'applicazione di sicurezza. Gli avvisi vengono generati quando: » Non viene rilevato nessun antivirus, antispyware o firewall. » Viene rilevato un antivirus o antispyware falso. » Le definizioni antivirus o antispyware non sono aggiornate. » Il monitoraggio antivirus o antispyware in tempo reale è disattivato. » Il prodotto antivirus o antispyware è scaduto. » Il prodotto antivirus o antispyware rileva il malware sui computer scansionati. » Il firewall è disabilitato. » Timeout HTTP/FTP durante il controllo di aggiornamenti del prodotto sui siti remoti: Questa opzione genera un avviso se viene superato il numero di secondi definiti per il timeout.

Opzione	Descrizione
Abilitazione/Disabilitazione dei controlli per le applicazioni di sicurezza	Per abilitare i controlli per le applicazioni di sicurezza installate in un profilo di scansione particolare: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Applicazioni**. 2. Fare clic sulla scheda **Opzioni avanzate**. 3. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**. 4. Selezionare la casella di controllo **Abilita scansione per le applicazioni installate sui computer di destinazione**. 5. (Scansioni senza agente) Selezionare la casella di controllo **Abilita controllo completo applicazioni di sicurezza per le scansioni senza agente**. **Nota** 1. Le scansioni senza agente eseguono temporaneamente un servizio piccolo sui computer remoti per recuperare le informazioni pertinenti. 2. La scansione delle applicazioni di sicurezza può essere configurata in un profilo di scansione in modo specifico per quel profilo. Assicurarsi di abilitare la scansione delle applicazioni di sicurezza in tutti i profili all'interno dei quali è necessaria. 3. Il numero di applicazioni di sicurezza supportate viene costantemente aggiornato. Per ottenere la versione più recente dell'elenco, fare clic sul collegamento disponibile. Configurazione delle applicazioni di sicurezza - Opzioni avanzate. Per configurare i trigger di avviso per le applicazioni di sicurezza installate in un profilo di scansione particolare: 1. Dalla scheda **Opzioni di controllo rete e sicurezza**, fare clic sulla sottoscheda **Applicazioni**. 2. Fare clic sulla scheda **Opzioni avanzate**. 3. Selezionare il profilo di scansione che si desidera personalizzare dal riquadro di sinistra sotto **Profili**. 4. Selezionare la casella di controllo **Abilita scansione per le applicazioni installate sui computer di destinazione**. 5. (Scansioni senza agente) Selezionare la casella di controllo **Abilita controllo completo applicazioni di sicurezza per le scansioni senza agente**. 6. Dal riquadro in fondo a destra, selezionare il trigger che si desidera configurare, quindi scegliere tra **Sì** e **No** nell'elenco a discesa posto accanto al rispettivo trigger di avviso. **Nota** La scansione delle applicazioni di sicurezza può essere configurata in un profilo di scansione in modo specifico per quel profilo. Assicurarsi di abilitare la scansione delle applicazioni di sicurezza in tutti i profili all'interno dei quali è necessaria.

12.5 Configurazione delle opzioni di scansione di sicurezza

Usare la scheda **Opzioni di scansione** per configurare i parametri operativi del motore di scansione di sicurezza. I parametri sono configurabili in modo specifico per ciascun profilo e definiscono il modo in cui il motore di scansione esegue i controlli sulle destinazioni e invia le query di dati al sistema operativo.


GFI LanGuard 2012 Scanning Profiles Editor
Scanning Profiles
Discuss this version...
Profile categories:
Complete/Combination Scans
Vulnerability Assessment
Network & Software Audit
Profiles:
Full Vulnerability Assessment
Full Scan (Active)
Full Scan (Slow Networks)
Common Tasks:
New scanning profile...
Set Active
Rename...
Delete...
Help:
Scanning Profiles...
LanGuard Scripting...
Vulnerability Assessment Options
Network & Software Audit Options
Scanner Options
Specify network discovery and other parameters on how the scanner is to discover machines and output debug information.
Network Discovery Methods
NetBIOS queries Yes
SNMP queries Yes
Ping sweep Yes
Custom TCP discovery (e.g. 21, 25, 80)
Network Discovery Options
Scanning delay (default 100 ms) 100
Network discovery query responses timeout (default 500 ms) 500
Number of retries (default 1) 1
Include non-responsive computers No
Perform a TCP port probing in order to detect mobile devices No
Network Scanner Options
Scanning threads count 3
NetBIOS Query Options
Scope ID
SNMP Query Options
Load SNMP enterprise numbers Yes
Community strings (e.g. public, private) public, private
Global Port Query Options
TCP port scan query timeout (default 1500 ms) 1500
UDP port scan query timeout (default 600 ms) 600

Screenshot 146: Proprietà Profili di scansione: scheda Opzioni di scansione

Le opzioni configurabili comprendono time-out, tipi di query da eseguire durante il controllo delle destinazioni, numero di thread di scansione, portata SNMP delle query e altro.

Importante

Configurare questi parametri con estrema attenzione. Una configurazione errata può influenzare le prestazioni delle scansioni di sicurezza di GFI LanGuard.

Per configurare le opzioni dello scanner:

1. Da **Editor dei profili di scansione > Categorie di profilo**, selezionare la categoria contenente il profilo di scansione da modificare (esempio: **Scansioni complete/combinate**).

2. Dalla sezione **Profili**, selezionare il profilo di scansione da modificare (esempio: **Valutazione completa delle vulnerabilità**).

3. Dal riquadro di destra fare clic su **Impostazioni scanner**.

4. Configurare i seguenti parametri che determinano il comportamento di scansione di GFI LanGuard:

Table 82: Opzioni scanner

Parametro	Descrizione
Metodi di individuazione della rete	
Query NetBIOS	Abilita/disabilita l'utilizzo di query NetBios per la rilevazione delle periferiche di rete.
Query SNMP	Abilita/disabilita l'utilizzo di query SNMP per la rilevazione delle periferiche di rete.

Parametro	Descrizione
Ping sweep	Abilita/disabilita l'utilizzo di ping sweep per la rilevazione delle periferiche di rete.
Individuazione TCP personalizzata	Individua la presenza di computer online inviando una query alle porte TCP aperte specificate.
Opzioni individuazione rete	
Ritardo di scansione	Immettere l'intervallo di tempo (in millisecondi) tra una scansione e l'altra.
Timeout risposte alle query per individuare la rete	Quantità di tempo in millisecondi di attesa di security scanner prima della scadenza durante un'interrogazione di un computer con query (NetBIOS/SNMP/Ping).
Numero di tentativi	Numero di tentativi di connessione di security scanner a un computer che non risponde prima di passare al computer successivo.
Comprende i computer che non rispondono	Esegui le scansioni su tutti i PC senza tenere conto del fatto che risultino online o meno.
Per rilevare i dispositivi mobili, effettuare un sondaggio delle porte TCP	Per rilevare i dispositivi mobili utilizzando le porte note, effettuare un sondaggio delle porte TCP.
Opzioni scanner di rete	
Conteggio thread scansione	Immettere il numero di thread di scansione che possono essere eseguiti in contemporanea.
Opzioni query Netbios	
ID scopo	Usato negli ambienti NETBIOS che richiedono un ID di scopo specifico per consentire l'interrogazione.
Opzioni query SNMP	
Carica numeri SNMP enterprise	Specifica se il security scanner debba utilizzare l'OID (Object Identifier database) contenente l'ID a mappa fornitori per identificare i vari tipi di dispositivi.
Stringa comunità	Specifica se il security scanner debba usare la stringa comunità specificata per il rilevamento del server SNMP e il recupero dei dati.
Opzioni globali query porta	
Timeout query di scansione porta TCP	Quantità di tempo in millisecondi di attesa del security scanner durante una scansione della porta TCP prima che il processo scada e lo scanner passi alla porta successiva.
Timeout query di scansione porta UDP	Quantità di tempo in millisecondi di attesa del security scanner durante una scansione della porta UDP prima che il processo scada e lo scanner passi alla porta successiva.
Opzioni WMI	
Timeout WMI	Quantità di tempo in millisecondi di attesa del security scanner di una risposta dal server WMI remoto prima che il processo scada e lo scanner passi all'elemento successivo.
Opzioni SSH	
Timeout SSH	Quantità di tempo in millisecondi di attesa del security scanner di una risposta dallo script SSH prima che il processo scada e lo scanner passi all'elemento successivo.
Porta SSH alternativa	Porte SSH alternative da utilizzare quando la porta predefinita 22 è irraggiungibile.
Finestra attività scanner	
Tipo di esito attività scanner	Modalità progresso attività: semplice (progresso di base: avvio/arresto delle operazioni) o verbose (informazioni più dettagliate sul flusso di processo).
Visualizza pacchetti ricevuti	Pacchetti TCP in uscita in formato grezzo, come sono stati ricevuti da security scanner.
Visualizza pacchetti inviati	Pacchetti TCP in uscita in formato grezzo, come sono stati inviati da security scanner.
Opzioni recupero informazioni sistema operativo	
Creare condivisione personalizzata se le condivisioni amministrative sono disabilitate	Se le condivisioni amministrative sono disabilitata, lo scanner creerà temporaneamente una condivisione nascosta sotto forma di <random GUID>$. La condivisione viene utilizzata per recuperare i dati che aiutano a identificare le vulnerabilità e le patch mancanti.
Avvia registro di sistema remoto	Se il servizio registro di sistema remoto viene arrestato sul computer scannerizzato, abilitare questa opzione per aprirlo temporaneamente durante la scansione di sicurezza.

13 Programmi di utilità

GFI LanGuard offre una serie di utility di rete che consentono il monitoraggio dell'attività di rete, la raccolta delle informazioni di rete e il controllo dei dispositivi di rete.

Argomenti del presente capitolo:

13.1 Ricerca DNS 220
13.2 Traceroute 223
13.3 Whois 224
13.4 Enumera computer 225
13.5 Enumera utenti 227
13.6 Controllo SNMP 228
13.7 Esplorazione SNMP 229
13.8 Controllo SQL Server® 230
13.9 Strumenti riga di comando 231

13.1 Ricerca DNS

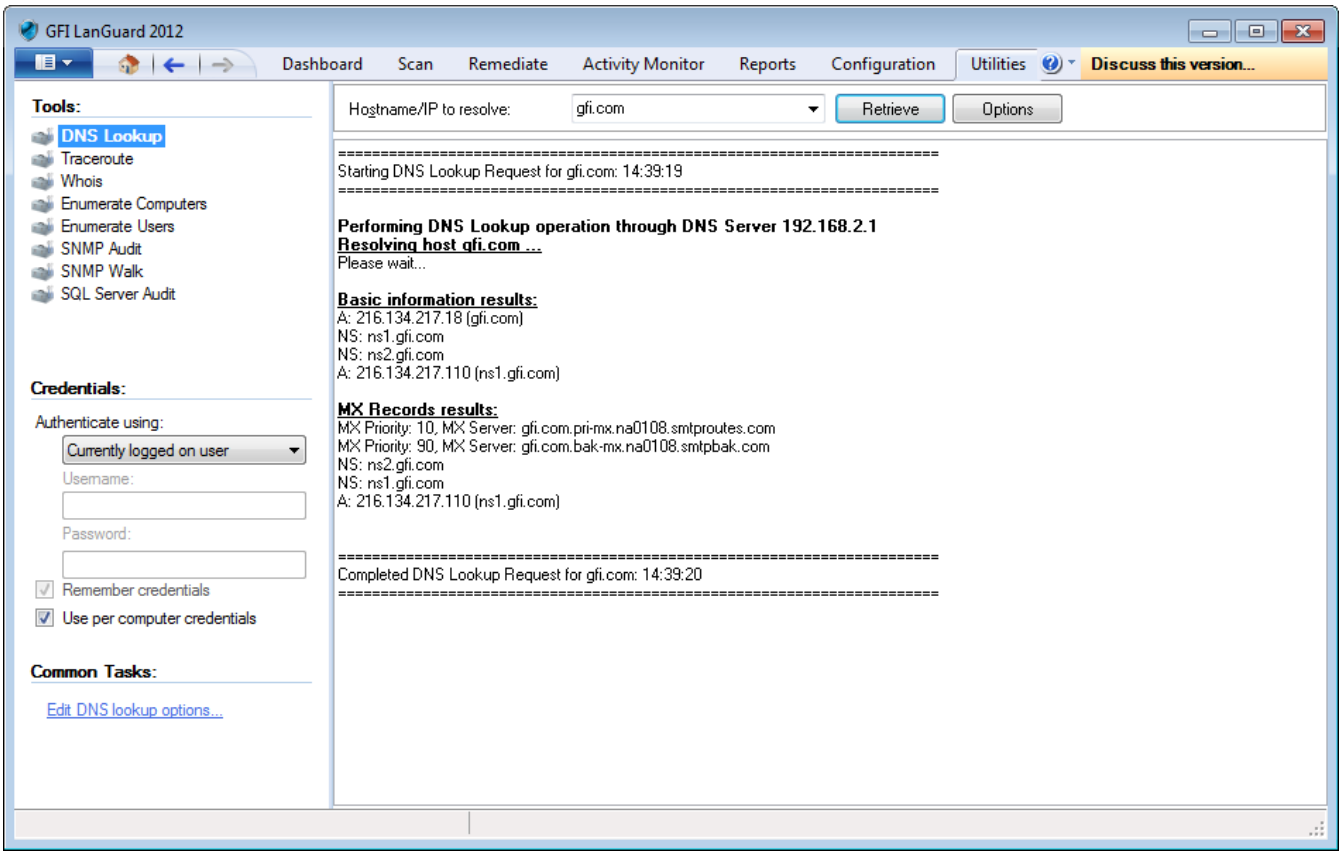
La ricerca DNS risolve i nomi di dominio nell'indirizzo IP corrispondente e recupera particolari informazioni dal dominio di destinazione (ad esempio, registro MX, ecc.).

Per risolvere un nome host/di dominio:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Programmi di utilità** e selezionare **Ricerca DNS** nel riquadro di sinistra sotto **Strumenti**.

3. Specificare il nome host da risolvere nella casella di testo **Nome host/IP da risolvere**.



Screenshot 147: Strumento Ricerca DNS

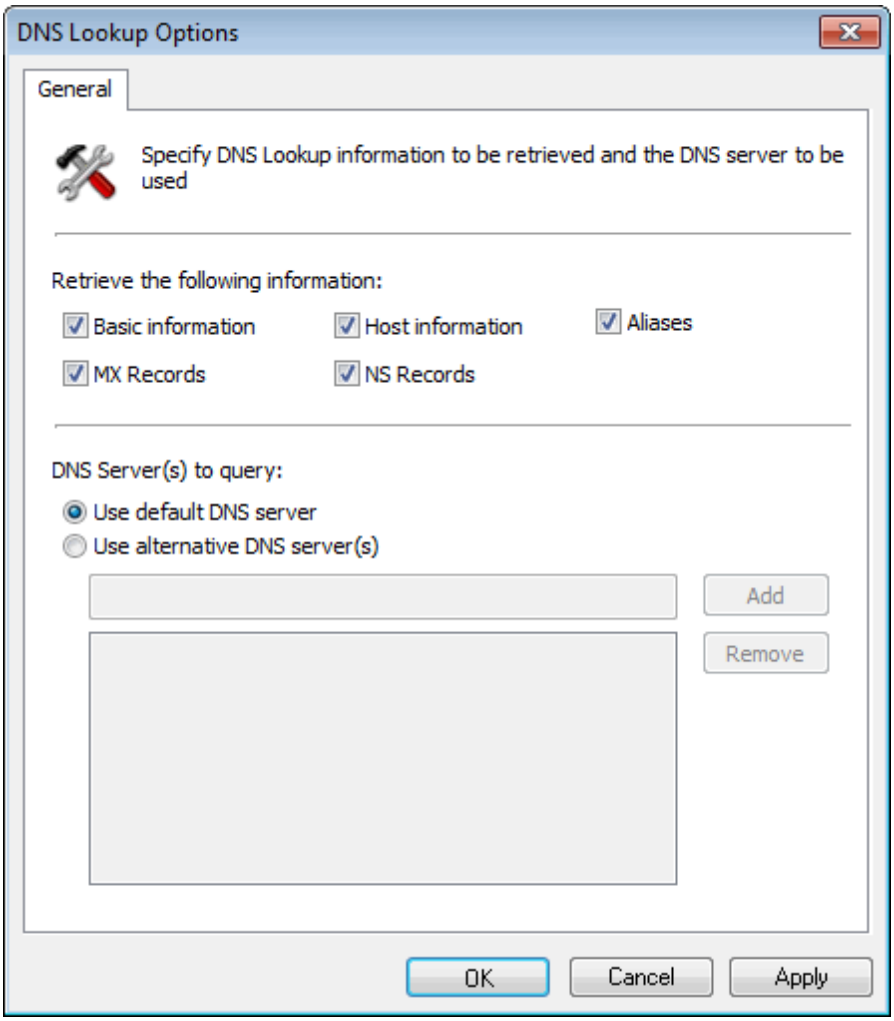
4. Sotto **Attività comuni** nel riquadro di sinistra, fare clic su **Modifica opzioni di ricerca DNS** o sul pulsante **Opzioni** nel riquadro di destra e specificare le informazioni riportate di seguito:

Table 83: Opzioni di ricerca DNS

Opzione	Descrizione
Informazioni di base	Recupera il nome host e il relativo indirizzo IP.
Informazioni host	Recupera i dettagli HINFO. Le informazioni host (conosciute come HINFO) solitamente includono informazioni sul computer di destinazione come le specifiche hardware e i dettagli sul sistema operativo.
Alias	Recupera le informazioni sui “Record A” configurati nel dominio di destinazione.
Record MX	Enumera tutti i server di posta e l'ordine (ossia la priorità) in cui ricevono ed elaborano i messaggi di posta elettronica per il dominio di destinazione.
Record NS	Specifica il “nome-server” dotato di autorità per un particolare dominio o sottodominio.

Nota

Alcune voci DNS non contengono queste informazioni per motivi di sicurezza.



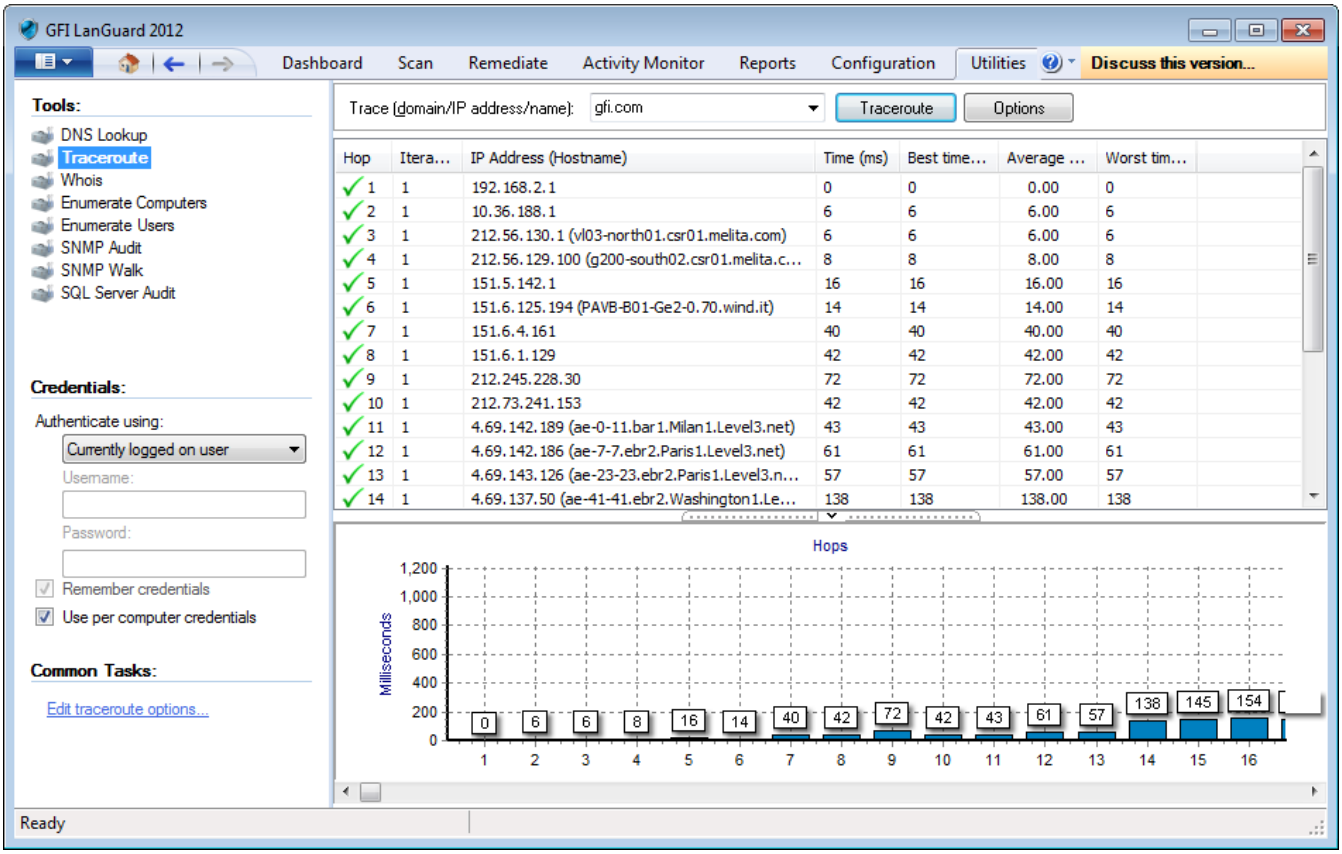
Screenshot 148: Opzioni Strumento Ricerca DNS

5. (Facoltativo) Specificare il server DNS alternativo al quale lo strumento di ricerca DNS invierà la query o lasciare il valore predefinito per usare il server DNS predefinito.

6. Fare clic su **Recupera** per iniziare il processo.

13.2 Traceroute

Traceroute identifica il percorso seguito da GFI LanGuard per raggiungere un computer di destinazione.



Screenshot 149: Strumento Traceroute

Per utilizzare lo strumento traceroute:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Programmi di utilità** e selezionare **Traceroute** nel riquadro di sinistra sotto **Strumenti**.

3. Nel menu a discesa **Traccia (dominio/IP/nome)**, specificare il nome/IP o il dominio da raggiungere.

4. (Facoltativo) Sotto **Attività comuni** nel riquadro di sinistra, fare clic su **Modifica opzioni Traceroute** o su **Opzioni** nel riquadro di destra per modificare le opzioni predefinite.

5. Fare clic sul pulsante **Traceroute** per avviare il processo di tracciatura.

Traceroute suddividerà il percorso verso un computer di destinazione in “hop”. Un hop indica una fase e rappresenta un computer attraversato durante il processo.

Le informazioni enumerate da questo strumento comprendono l'IP dei computer attraversati, il numero di volte in cui un computer è stato attraversato e il tempo impiegato per raggiungere il rispettivo computer. Vicino a ciascun hop viene inoltre inserita un'icona. Questa icona indica lo stato di quel particolare hop. Le icone usate in questo strumento comprendono:

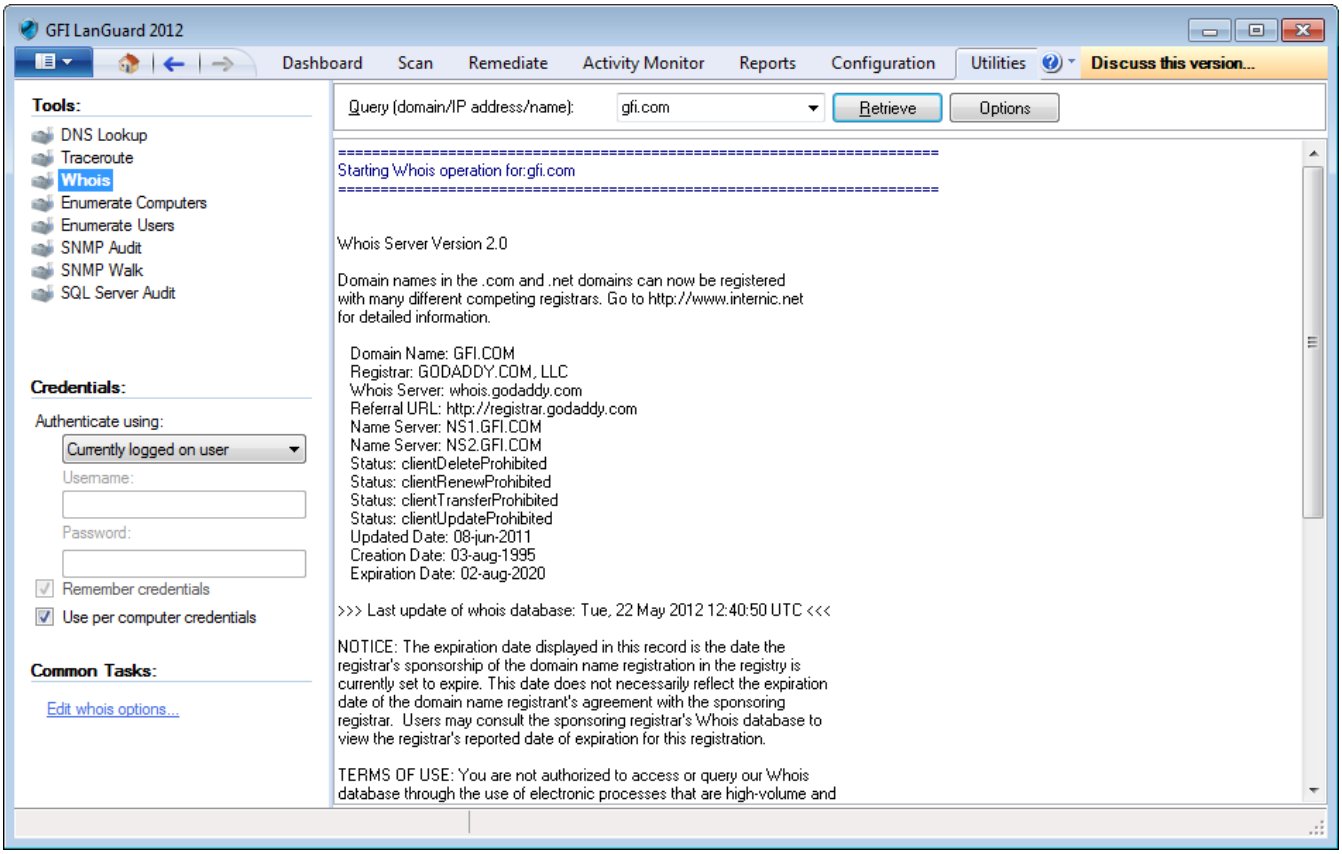
Table 84: Icone Traceroute

Icona	Descrizione
✓	Indica un hop avvenuto correttamente con parametri normali.

Icona	Descrizione
	Indica un hop avvenuto correttamente, ma che ha richiesto tempi più lunghi del previsto.
	Indica un hop avvenuto correttamente, ma che ha richiesto tempi troppo estesi.
	Indica che l'hop è scaduto (> 1000 ms)

13.3 Whois

Il Whois ricerca informazioni all'interno di un particolare dominio o indirizzo IP.



Screenshot 150: Strumento Whois

1. Avviare GFI LanGuard.

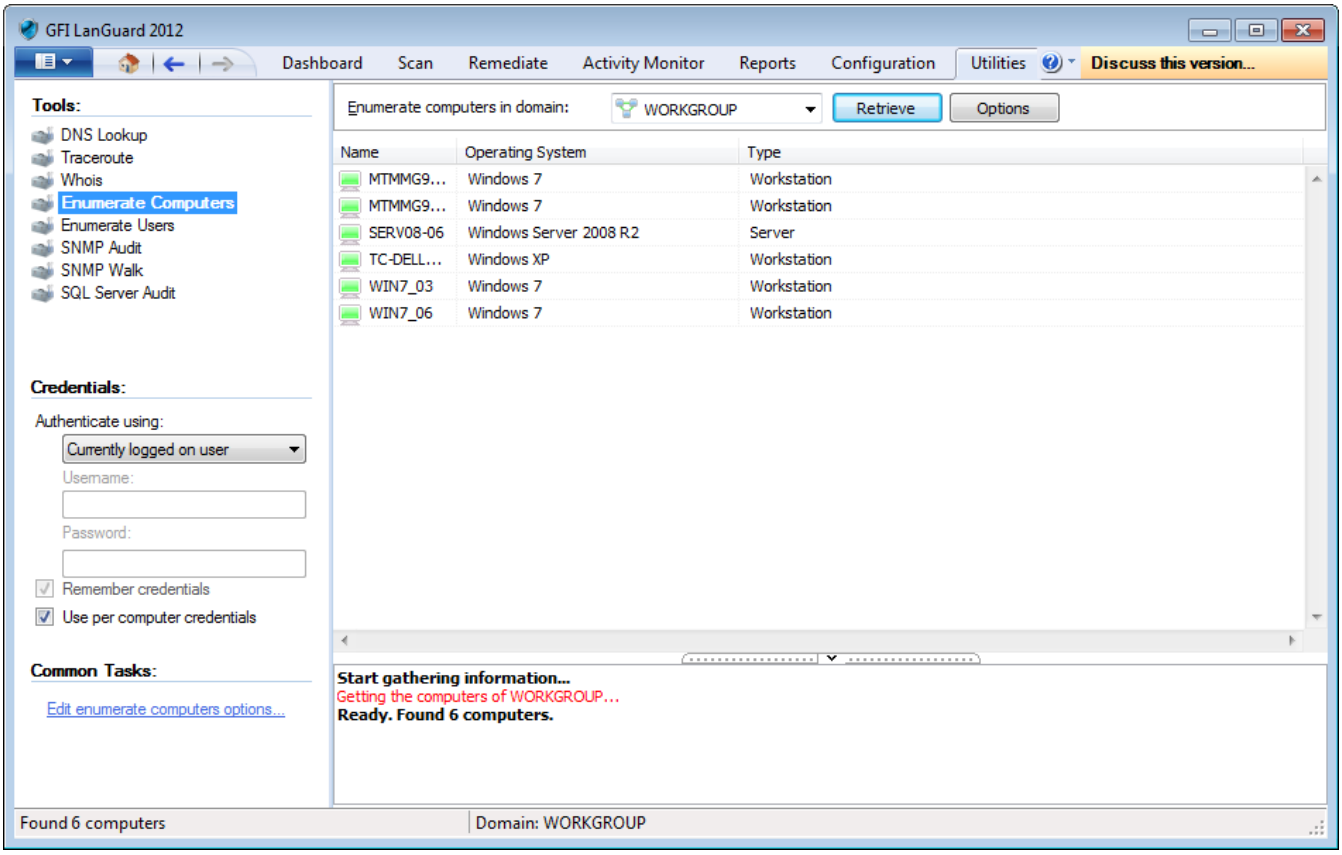
2. Fare clic sulla scheda **Programmi di utilità** e selezionare **Whois** nel riquadro di sinistra sotto **Strumenti**.

3. Nel menu **Query (dominio/IP/nome)**, specificare il nome/IP o il dominio da raggiungere.

4. (Facoltativo) Sotto **Attività comuni** nel riquadro di sinistra, fare clic su **Modifica opzioni Whois** o su **Opzioni** nel riquadro di destra per modificare le opzioni predefinite.

5. Fare clic su **Recupera** per iniziare il processo.

13.4 Enumera computer



Screenshot 151: Strumento Enumera computer

Il programma di utilità Enumera computer identifica i domini e i gruppi di lavoro di una rete. Durante l'esecuzione, questo strumento eseguirà la scansione su ciascun dominio/gruppo di lavoro rilevato enumerando i rispettivi computer.

- Le informazioni enumerate da questo strumento comprendono:
- nome del dominio o del gruppo di lavoro
- elenco di computer del dominio/gruppo di lavoro
- sistema operativo installato sui computer rilevati
- Qualsiasi dettaglio aggiuntivo che possa essere recuperato tramite il NetBIOS.

I computer vengono enumerati utilizzando uno dei seguenti metodi:

Table 85: Opzioni di Enumera computer

Opzione	Descrizione
Da Active Directory®	Questo metodo è il più veloce e includerà i computer attualmente spenti.
Da Windows Explorer	Questo metodo enumera i computer per mezzo di una scansione in tempo reale sulla rete ed è pertanto più lento e non includerà i computer spenti.

Per enumerare i computer:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Programmi di utilità** e selezionare **Enumera computer** nel riquadro di sinistra sotto **Strumenti**.

3. Da **Enumera i computer nel dominio** , selezionare il dominio desiderato.

4. Da **Attività comuni** nel riquadro di sinistra, fare clic su **Modifica opzioni di enumerazione dei computer** o su **Opzioni** nel riquadro di destra.

5. Selezionare se enumerare i computer da Active Directory® o da Risorse del computer.

6. Fare clic su **Recupera** per iniziare il processo.

> **Nota**
>
> Per una scansione di Active Directory®, sarà necessario eseguire lo strumento all'interno di un account dotato di diritti di accesso ad Active Directory®.

13.4.1 Avvio di una scansione di sicurezza

Per avviare una scansione di sicurezza direttamente dallo strumento "Enumera computer", fare clic con il tasto destro del mouse su uno dei computer enumerati e selezionare Scansiona.

È anche possibile lanciare una scansione di sicurezza e allo stesso tempo continuare a usare lo strumento Enumera computer. A tal fine, fare clic con il tasto destro del mouse su uno dei computer enumerati e selezionare Scansione in Background.

13.4.2 Distribuzione di patch personalizzate

È possibile usare lo strumento Enumera computer per distribuire patch personalizzate e software di terze parti sui computer enumerati. Per avviare un processo di distribuzione direttamente da questo strumento:

1. Selezionare i computer sui quali eseguire la distribuzione.

2. Fare clic con il tasto destro del mouse su uno dei computer selezionati e selezionare **Distribuisci patch personalizzate**.

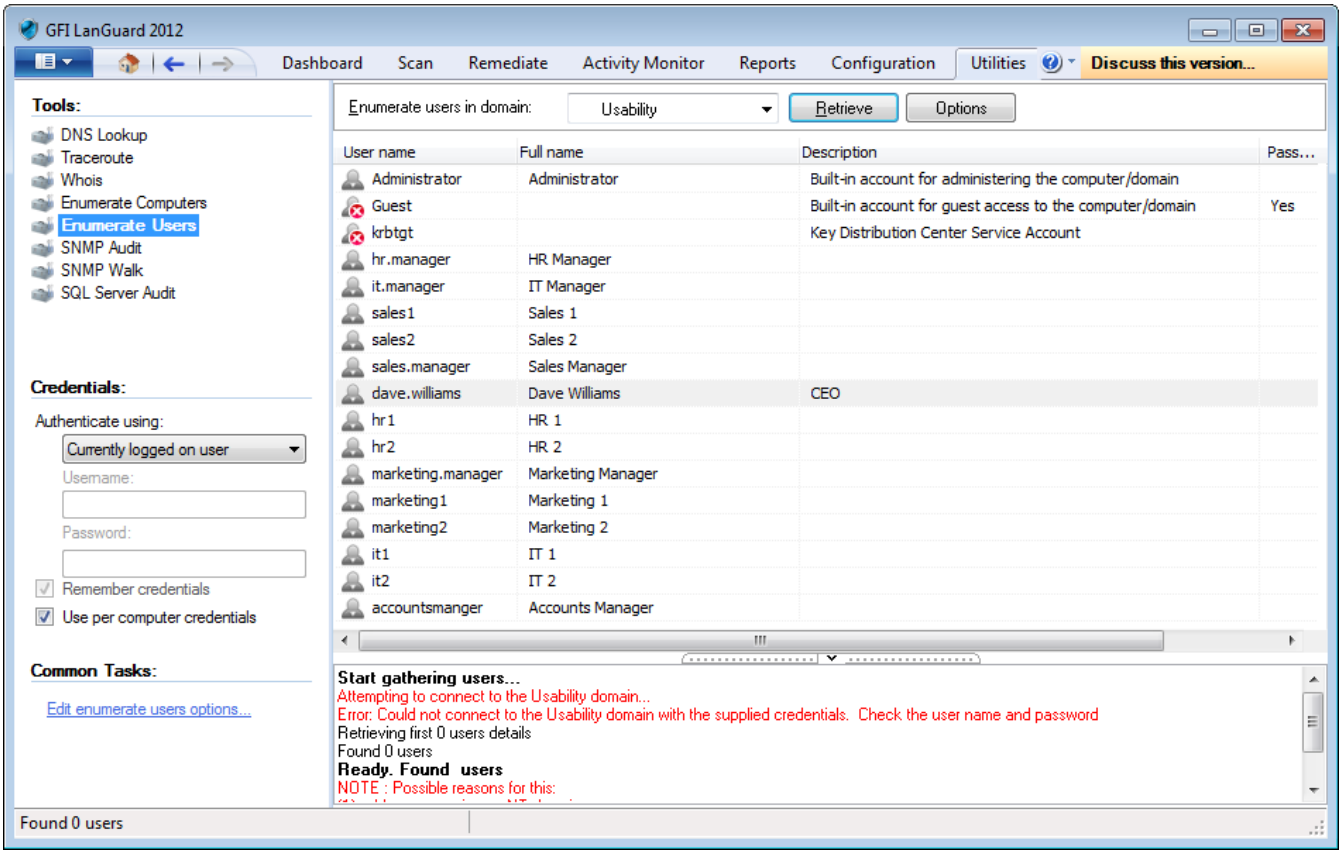
13.4.3 Abilitazione dei criteri di controllo

Lo strumento Enumera computer consente di configurare i criteri di controllo per particolari computer. A tal fine procedere come segue:

1. Selezionare i computer sui quali abilitare i criteri di controllo.

2. Fare clic con il tasto destro del mouse su uno dei computer selezionati e selezionare **Abilita criteri di controllo**. Il sistema avvierà la **procedura guidata di configurazione dei criteri di controllo** che guiderà l'utente durante il processo di configurazione.

13.5 Enumera utenti



Screenshot 152: Finestra di dialogo dello strumento Enumera utenti

Per eseguire la scansione di Active Directory® e recuperare l'elenco di tutti gli utenti e i contatti inclusi in questo database:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Programmi di utilità** e selezionare **Enumera utenti** nel riquadro di sinistra sotto **Strumenti**.

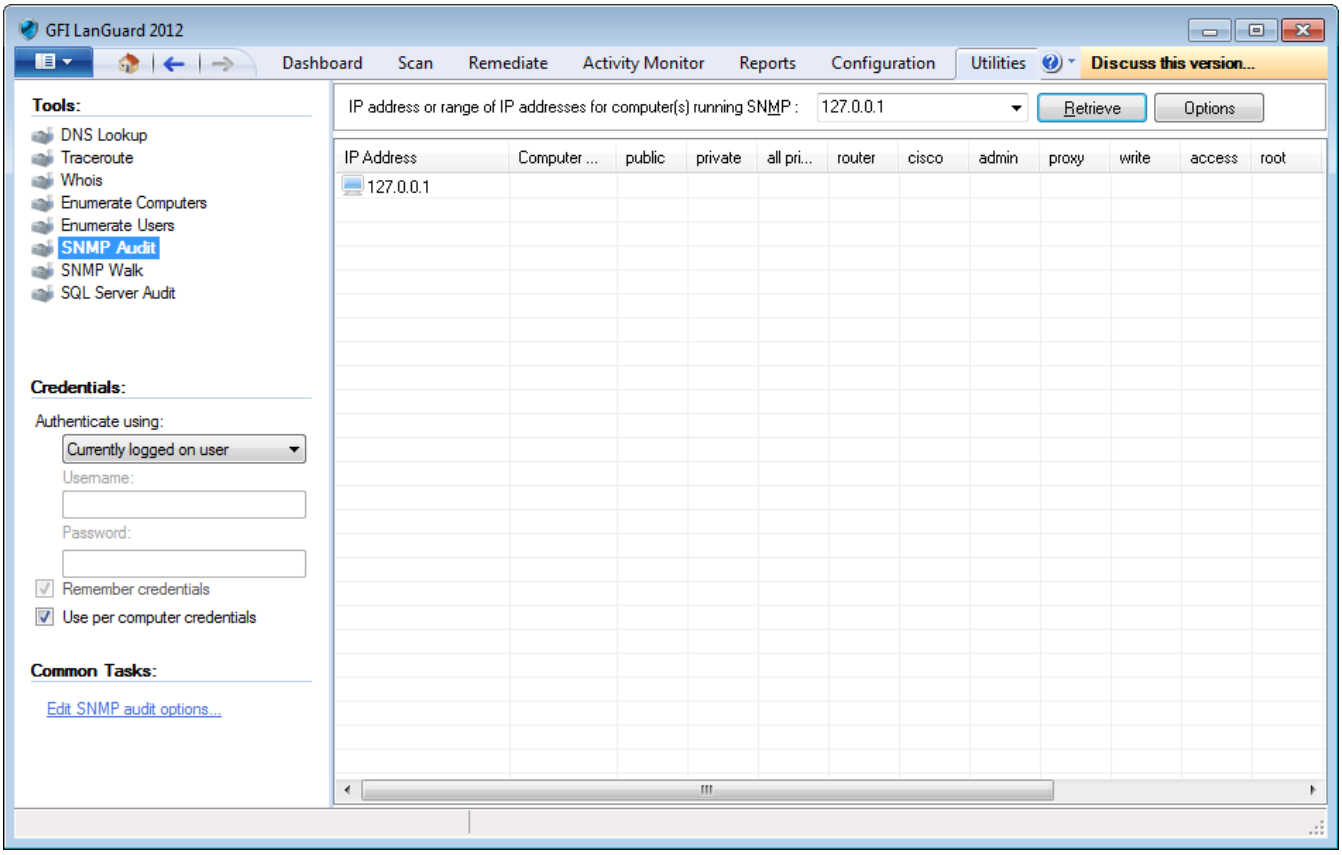
3. Dal menu **Enumera gli utenti nel dominio**, selezionare il dominio desiderato.

4. Da **Attività comuni** nel riquadro di sinistra, fare clic su **Modifica opzioni di enumerazione degli utenti** o su **Opzioni** nel riquadro di destra per filtrare le informazioni da estrarre e visualizzare solo i dettagli degli utenti o dei contatti. Inoltre, è possibile configurare questo strumento in modo da evidenziare gli account disabilitati o bloccati.

5. Fare clic su **Recupera** per iniziare il processo.

> **Nota**
>
> Questo strumento può abilitare o disabilitare gli account utente enumerati. Fare clic con il tasto destro del mouse sull'account e selezionare **Abilitare/disabilitare account** in base alla necessità.

13.6 Controllo SNMP



Screenshot 153: Strumento Controllo SNMP

Questo strumento identifica e segnala le stringhe comunità SNMP deboli lanciando un attacco al dizionario utilizzando i valori memorizzati nel file di dizionario predefinito (snmp-pass.txt).

È possibile aggiungere nuove stringhe comunità al file di dizionario predefinito utilizzando un editor di testo (ad esempio blocconote.exe).

È anche possibile configurare lo strumento Controllo SNMP in modo da utilizzare altri file di dizionario. A tal fine, specificare il percorso del file di dizionario desiderato nella sezione opzioni dello strumento a destra della console di gestione.

Per eseguire i controlli SNMP sulle destinazioni di rete e identificare le stringhe comunità deboli:

1. Avviare GFI LanGuard.

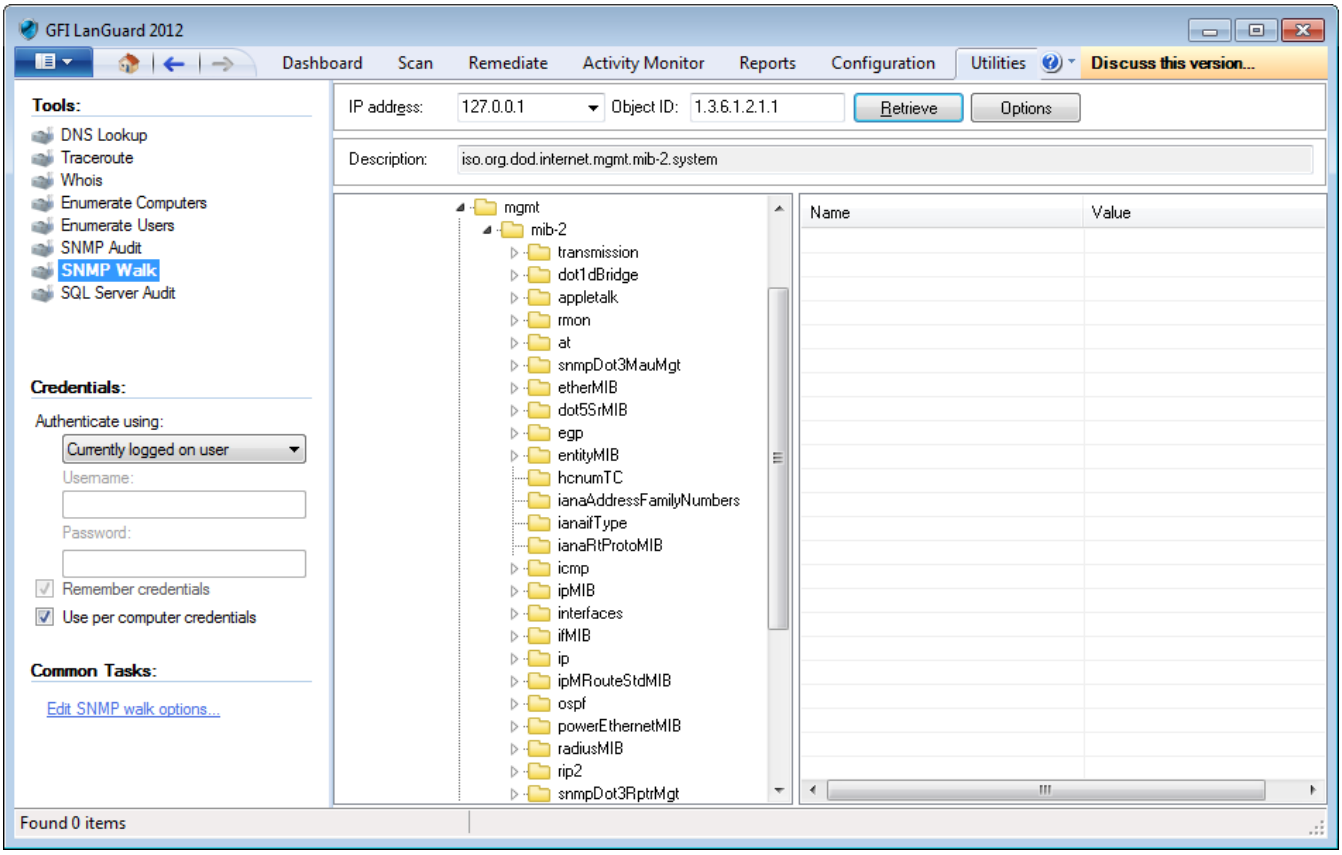
2. Fare clic sulla scheda **Programmi di utilità** e selezionare **Controllo SNMP** nel riquadro di sinistra sotto **Strumenti**.

3. Nell'elenco a discesa **IP del computer sul quale è in esecuzione SNMP**, specificare l'IP da raggiungere.

4. Da **Attività comuni** nel riquadro di sinistra, fare clic su **Modifica opzioni di controllo SNMP** o su **Opzioni** nel riquadro di destra per modificare le opzioni predefinite.

5. Fare clic su **Recupera** per iniziare il processo.

13.7 Esplorazione SNMP



Screenshot 154: Strumento esplorazione SNMP

Per sondare i nodi della rete e recuperare le informazioni SNMP (ad esempio, OID):

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Programmi di utilità** e selezionare Esplorazione SNMP nel riquadro di sinistra sotto **Strumenti**.

3. Nel menu a discesa **Indirizzo IP**, specificare l'indirizzo IP del computer sul quale eseguire la scansione per trovare le informazioni SNMP.

4. Da **Attività comuni** nel riquadro di sinistra, fare clic su **Modifica opzioni di esplorazione SNMP** o su **Opzioni** nel riquadro di destra per modificare le opzioni predefinite, ad esempio per fornire stringhe comunità alternative.

5. Fare clic su **Recupera** per iniziare il processo.

IMPORTANTE

Le attività SNMP spesso vengono bloccate dal router/firewall in modo da impedire agli utenti di Internet di eseguire la scansione SNMP sulla propria rete. Gli utenti malintenzionati possono sfruttare le informazioni enumerate dalla scansione SNMP per introdursi in modo illecito nella rete/sistemi dell'utente. A meno che il servizio sia necessario, si consiglia fortemente di disattivare SNMP.

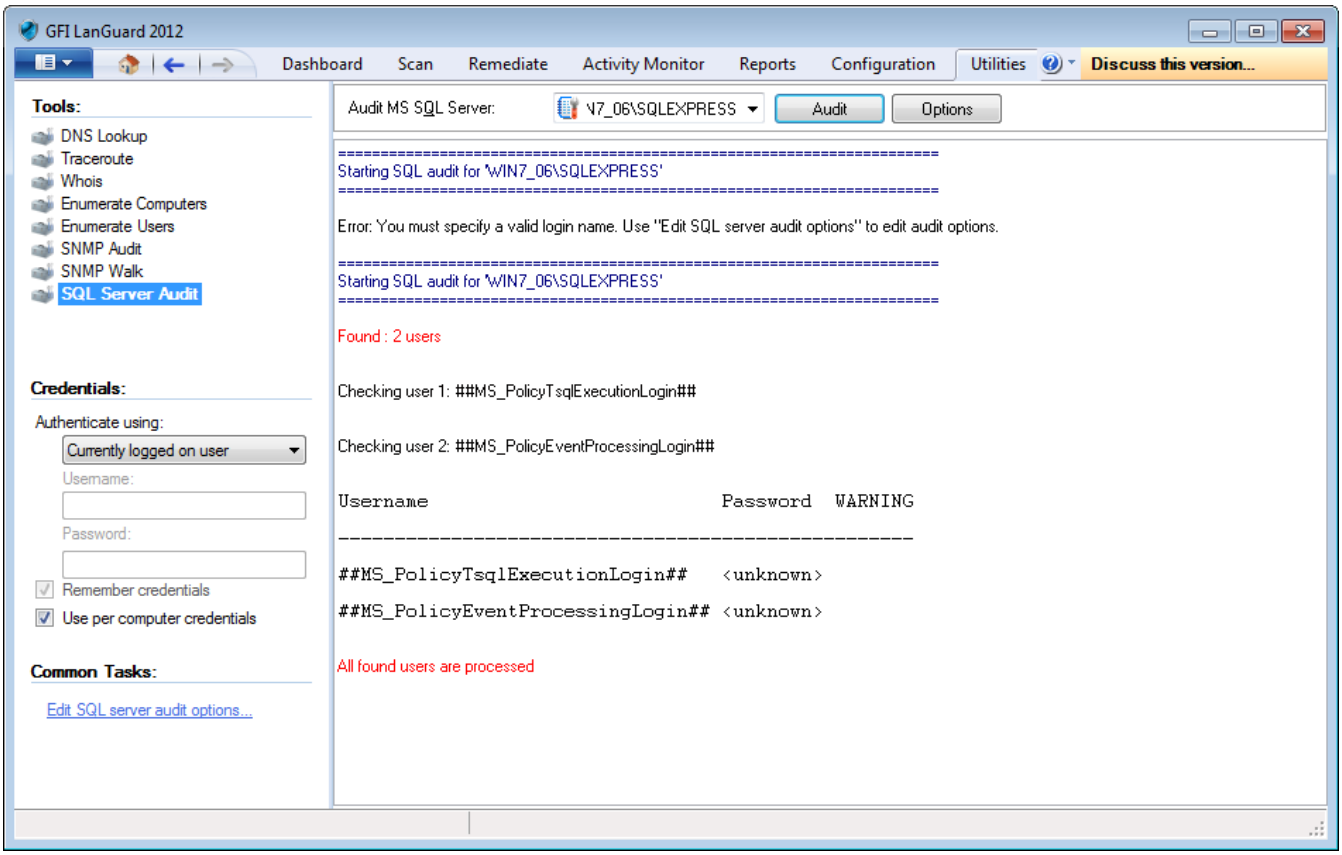
13.8 Controllo SQL Server®

Questo strumento consente di testare la vulnerabilità delle password dell'account 'sa' (vale a dire, amministratore root) e degli altri account utente SQL configurati su SQL Server®. Durante il processo di controllo, questo strumento lancerà attacchi al dizionario sugli account di SQL Server® utilizzando le credenziali specificate nel file di dizionario 'password.txt'. È anche possibile configurare lo strumento Controllo SQL Server® in modo da utilizzare altri file di dizionario. È possibile personalizzare i file di dizionario aggiungendo nuove password all'elenco predefinito.

Per eseguire un controllo di protezione su una particolare installazione di SQL Server®:

1. Avviare GFI LanGuard.

2. Fare clic sulla scheda **Programmi di utilità** e selezionare **Controllo SQL Server** nel riquadro di sinistra sotto **Strumenti**.



Screenshot 155: Controllo SQL Server®

3. Nel menu **Controlla MS SQL Server** specificare l'indirizzo IP del server SQL Server® che si desidera controllare.

4. Da **Attività comuni** nel riquadro di sinistra, fare clic su **Modifica opzioni di controllo SQL Server®** o sul pulsante **Opzioni** nel riquadro di destra per modificare le opzioni predefinite come l'avvio di attacchi al dizionario su tutti gli altri account utente SQL.

5. Fare clic su **Controllo** per iniziare il processo.

13.9 Strumenti riga di comando

Gli strumenti della riga di comando consentono di lanciare scansioni delle vulnerabilità della rete e sessioni di distribuzione delle patch, nonché di importare ed esportare profili e vulnerabilità senza caricare la console di gestione GFI LanGuard. Utilizzare le informazioni contenute in questa sezione sulla modalità di esecuzione delle funzioni di gestione patch con gli strumenti CMD seguenti:

- Lnsscmd.exe
- Deploycmd.exe
- Impex.exe

13.9.1 Utilizzo di lnsscmd.exe

Lo strumento di scansione delle destinazioni della linea di comando "lnsscmd.exe" consente di eseguire controlli di vulnerabilità sulle destinazioni di rete direttamente dalla linea di comando o tramite applicazioni di terzi, file batch e script. Lo strumento della linea di comando "lnsscmd.exe" supporta i seguenti parametri:

```
lnsscmd <Target> [/profile=profileName] [/report=reportPath]
[/reportname=reportName] [/output=pathToXmlFile] [/user=username
/password=password] [/Email [/EmailAddress=EmailAddress]]
[/DontShowStatus] [/UseComputerProfiles] [/Wake] [/Shutdown
[/ShutdownIntervalStart=<hh:mm:ss>] [/ShutdownIntervalEnd=<hh:mm:ss>]]
[/?]
```

parametri di comando lnsscmd

Table 86: Parametri di comando insscmd

Parametro	Descrizione
Destinazione	Specificare l'indirizzo IP/l'intervallo di IP o il/i nome/i degli host da sottoporre a scansione.
/Profile	(Facoltativo) Specificare il profilo di scansione che verrà utilizzato durante una scansione di sicurezza. Se questo parametro non è specificato, verrà utilizzato il profilo di scansione attualmente attivo in GFI LanGuard. **Nota** Nella console di gestione, il profilo di scansione predefinito (ossia il profilo attualmente attivo) è indicato dalla parola (Attivo) accanto al relativo nome. Per visualizzare il profilo attivo, espandere la scheda **Configurazione** nodo > **Profili di scansione**.
/Output	(Facoltativo) Specificare il percorso completo (compreso il nome file) del file XML in cui verranno salvati i risultati della scansione.
/Report	(Facoltativo) Directory o nome completo del file per l'output del rapporto di scansione.
/ReportName	(Facoltativo) Nome del rapporto da generare. Se non indicato, il rapporto verrà salvato con un nome predefinito.
/User e /Password	(Facoltativo) Specificare le credenziali alternative che il motore di scansione utilizzerà per l'autenticazione su un computer di destinazione durante la scansione di sicurezza. In alternativa, è possibile utilizzare il parametro /UseComputerProfiles per avvalersi delle credenziali di autenticazione già configurate nel dashboard.
/Email	(Facoltativo) Invia il rapporto risultante per posta elettronica. Verranno utilizzati l'indirizzo di posta elettronica e il server di posta specificati in **Configurazione > Opzioni di avviso**.
/EmailAddress	(Facoltativo) Dipende da **/Email**. Ignora opzioni generali di avviso e utilizza l'indirizzo di posta elettronica specificato.
/DontShowStatus	(Facoltativo) Includere questo parametro se si desidera eseguire una scansione invisibile all'utente. In questo modo, i dettagli sullo stato di avanzamento della scansione non verranno visualizzati.
/UseComputerProfiles	(Facoltativo) Utilizza credenziali computer se disponibili.

Parametro	Descrizione
/Wake	(Facoltativo) Attiva i computer non in linea.
/Shutdown	(Facoltativo) Arresta i computer dopo la scansione.
/ShutdownIntervalStart	(Facoltativo) Dipende da **/Shutdown**. L'orario di inizio dell'intervallo quando è consentito l'arresto. Utilizzare il formato hh:mm:ss.
/ShutdownIntervalEnd	(Facoltativo) Dipende da **/Shutdown**. L'orario di fine dell'intervallo quando è consentito l'arresto. Utilizzare il formato hh:mm:ss.
/?	(Facoltativo) Utilizzare questo parametro per mostrare le istruzioni relative all'uso degli strumenti della linea di comando.

Nota

Racchiudere sempre tra virgolette i percorsi completi e i nomi dei profili: Ad esempio, "`[percorso o nome percorso]`", o "`C:\temp\test.xml`".

Lo strumento di scansione delle destinazioni della linea di comando consente di inserire parametri mediante variabili specifiche. Queste variabili verranno sostituite automaticamente con il loro valore rispettivo durante l'esecuzione. La sottostante tabella illustra le variabili supportate:

Variabili supportate

Table 87: Variabili supportate in Inssmcd

Variabile	Descrizione
%INSTALLDIR%	Durante la scansione, questa variabile verrà sostituita dal percorso della directory di installazione di GFI LanGuard.
%TARGET%	Durante la scansione, questa variabile verrà sostituita dal nome del computer di destinazione.
%SCANDATE%	Durante la scansione, questa variabile verrà sostituita dalla data di scansione.
%SCANTIME%	Durante la scansione, questa variabile verrà sostituita dall'ora di scansione.

Esempio

1. Per eseguire una scansione di sicurezza su un computer di destinazione avente per indirizzo IP "130.16.130.1".

2. Salvare i risultati della scansione della scansione in "`c:\out.xml`" (ossia file XML).

3. Generare un rapporto PDF e salvarlo in '`c:\result.odf`'.

4. Inviare il rapporto PDF tramite posta elettronica a "lanss@domain.com".

Il comando deve essere come segue:

```
lnsscmd.exe 130.16.130.1 /Profile=”Predefinito" /Output="c:\out.xml"
/Report="c:\result.pdf" /Email /emailAddress="lanss@domain.com"
```

13.9.2 Utilizzo di deploycmd.exe

Lo strumento per la distribuzione di patch della riga di comando 'deploycmd.exe' consente di distribuire patch Microsoft® e software di terzi su destinazioni remote direttamente dalla riga di comando o tramite applicazioni di terzi, file batch o script. Lo strumento della linea di comando "deploycmd.exe" supporta i seguenti parametri:

```
deploycmd <destinazione> </file=Nome file> [/switches=Switch]
[/username=Nome utente /password=Password] [/warnuser] [/userapproval]
[/stopservices] [/customshare=Nome condivisione personalizzata] [/reboot]
[/rebootuserdecides] [/wake] [/shutdown] [/deletefiles] [/timeout=Timeout
```

```
(sec)] [/usecomputerprofiles] [/RebootCountdown=Time(sec)]
[/RebootCountdownMessage=”Messaggio personalizzato”]
[/RebootAtFirstOccurenceOf=Ora(formattata come "hh:mm:ss")]
[/ShutDownAtFirstOccurenceOf=Ora(formattata come "hh:mm:ss")]
[/RebootInInterval] [/ShutDownInInterval] [/RebootIntervalStart=Ora
(formattata come "hh:mm:ss")] [/RebootIntervalEnd=Ora(formattata come
"hh:mm:ss")] [/?]
```

Parametri di comando deploycmd

Table 88: Parametri di comando deploycmd

Parametro	Descrizione
Destinazione	Specificare il/i nome/i, l'indirizzo IP o l'intervallo di IP del/dei computer di destinazione nel/i quale/i verranno distribuite le patch.
/File	Specificare il file che si desidera distribuire nella/e destinazione/i specificata/e.
/User e /Password	(Facoltativo) Specificare le credenziali alternative che il motore di scansione utilizzerà per l'autenticazione su un computer di destinazione durante la distribuzione delle patch. In alternativa, è possibile utilizzare il parametro /UseComputerProfiles per avvalersi delle credenziali di autenticazione già configurate nel dashboard.
/warnuser	(Facoltativo) Includere questo parametro se si desidera informare l'utente del computer di destinazione che è in corso un'installazione di file/patch. Gli utenti verranno informati tramite la visualizzazione di un messaggio sullo schermo immediatamente prima dell'avvio della sessione di distribuzione.
/useraproval	(Facoltativo) Includere questo parametro per richiedere l'approvazione dell'utente prima di avviare il processo di installazione di file/patch. Questo consente agli utenti di posticipare il processo di installazione di file/patch (ad esempio, fino a quando non viene completato un processo già avviato sul computer di destinazione).
/stopservice	(Facoltativo) Includere questo parametro se si desidera arrestare determinati servizi sul computer di destinazione prima di installare il file o la patch. **Nota** Non è possibile specificare i servizi che verranno arrestati direttamente dallo strumento della linea di comando. I servizi possono essere aggiunti o rimossi solo tramite la console di gestione.
/customshare	(Facoltativo) Specificare la condivisione di destinazione in cui si desidera trasferire il file prima che venga installato.
/reboot	(Parametro facoltativo) Includere questo parametro se si desidera riavviare il computer di destinazione dopo la distribuzione di file/patch distribuzione di patch.
/rebootuserdecides	(Parametro facoltativo) Includere questo parametro per consentire all'utente del computer di destinazione in uso di decidere quando riavviare il computer (dopo l'installazione della patch).
/wake	Attiva i computer non in linea.
/shutdown	(Parametro facoltativo) Includere questo parametro se si desidera arrestare il computer di destinazione dopo aver installato il file/la patch.
/deletefiles	(Parametro facoltativo) Includere questo parametro se si desidera eliminare il file di origine dopo averne completato l'installazione.
/timeout	(Parametro facoltativo) Specificare il time-out dell'operazione di distribuzione. Questo valore definisce il tempo a disposizione per l'esecuzione del processo di distribuzione prima che l'installazione del file/della patch venga interrotta.
/usecomputerprofiles	(Facoltativo) Usa i dati dei profili computer.
/RebootCountdown	(Facoltativo) Mostra all’utente remoto una finestra di countdown di riavvio per il numero di secondi mancanti prima di procedere al riavvio.
/RebootCountdownMessage	(Facoltativo) Usato insieme a **/RebootCountdown**. Mostra un messaggio personalizzato all’utente remoto prima del riavvio del computer.

Parametro	Descrizione
/RebootAtFirstOccurenceOf	(Facoltativo) Riavvia il computer alla prima occorrenza di un orario specificato. Si prevede che l'ora sia in formato 24 ore "hh:mm:s s". Ad esempio, 18:30:00.
/ShutDownAtFirstOccurenceOf	(Facoltativo) Arresta il computer alla prima occorrenza di un orario specificato. Si prevede che l'ora sia in formato 24 ore "hh:mm:s s". Ad esempio, 18:30:00.
/RebootInInterval	(Facoltativo) Riavvia il computer dopo la distribuzione se questa viene completata entro l'intervallo di tempo specificato. In caso contrario, attendere di poter indicare manualmente l'intervallo. Sono richiesti i parametri `/RebootIntervalStart` e `/RebootIntervalEnd`.
/ShutdownIntervalStart	(Facoltativo) Dipende da **/Shutdown**. L'orario di inizio dell'intervallo quando è consentito l'arresto. Utilizzare il formato hh:mm:ss.
/ShutdownIntervalEnd	(Facoltativo) Dipende da **/Shutdown**. L'orario di fine dell'intervallo quando è consentito l'arresto. Utilizzare il formato hh:mm:ss.
/ShutDownInInterval	(Facoltativo) Arresta il computer dopo la distribuzione se questa viene completata entro l'intervallo di tempo specificato. In caso contrario, attendere di poter indicare manualmente l'intervallo.
/?	(Facoltativo) Utilizzare questo parametro per mostrare le istruzioni relative all'uso dello strumento della linea di comando.

Esempio

1. Distribuire un file denominato "patchA001002.XXX".

2. Il computer di destinazione è "TMJohnDoe".

3. Al termine della distribuzione del file, riavviare il computer di destinazione.

Il comando deve essere come segue:

```
deploycmd TMJohnDoe /file="patchA001002.XXX" /reboot
```

13.9.3 Utilizzo di impex.exe

Impex è uno strumento della linea di comando che può essere utilizzato per importare ed esportare profili e vulnerabilità da GFI LanGuard Network Security Scanner. I parametri supportati da questo strumento sono i seguenti:

```
impex [[/H] | [/?]] | [/XML:xmlfile [/DB:dbfile] [[/EX] [/MERGE]] | [/IM
[/ONLYNEWER]] [/PROFILES | /VULNS | /PORTS | /PROFILE:name | /VULNCAT:cat
[/VULN:name] | /PORTTYPE:type [/PORT:number]] [/SKIP | /OVERWRITE |
/RENAME:value]]
```

Switch di comando impex

Table 89: Switch di comando impex

Parametro	Descrizione
/H **/?** **Esegui impex senza parametri**	Visualizza le informazioni della guida.
/XML:<xmlfile>	Questo parametro specifica il nome del file XML importato o esportato. <xmlfile> deve essere sostituito con il nome del file in cui viene esportato il profilo. **Nota** Questo parametro è obbligatorio per importare o esportare avvisi.
/DB:<dbfile>	Dove <dbfile> è il file del database da usare durante l'operazione di importazione/esportazione. Se questo valore non è specificato, verrà usato il file predefinito "operationsprofiles.mdb".
/EX	Esporta dati dal database nel file XML (Opzione predefinita).

Parametro	Descrizione
/MERGE	Se viene specificato questo valore quando l'XML di destinazione da esportare esiste già, il file verrà aperto e i dati verranno riuniti; in caso contrario il file XML viene eliminato.
/IM	Importa i dati dal file XML nel database
/ONLYNEWER	Quando viene specificato questo valore, solo le vulnerabilità più recenti dell'ultima vulnerabilità presente nel database verranno importate.
/PROFILES	Esporta/importa tutti i profili di scansione.
/VULNS	Esporta/importa tutte le vulnerabilità.
/PORTS	Esporta/importa tutte le porte
/PROFILE:<name>	Esporta/importa il profilo di scansione specificato.
/VULNCAT:<category>	Esporta/importa tutte le vulnerabilità della categoria specificata.
/VULN:<name>	Esporta/importa la vulnerabilità specificata (/VULNCAT deve essere specificato).
/PORTTYPE:<type>	Esporta/importa tutte le porte del tipo specificato.
/PORT:<number>	Esporta/importa la porta specificata (/PORTTYPE deve essere specificato).
/SKIP	Se un elemento esiste già nel database/XML di destinazione, quel dato elemento verrà ignorato.
/OVERWRITE	Se un elemento esiste già nel database/XML di destinazione, quel dato elemento verrà sovrascritto.
/RENAME:<value>	Se un elemento esiste già nel database/XML di destinazione, quel dato elemento verrà rinominato <value>. Se sono stati specificati /PROFILE o /VULN, i dati sulla porta verranno riuniti nel caso in cui l'elemento sia una porta o rinominati e al nome dell'elemento verrà anteposto <value> in tutti gli altri casi.

Esempio 1

Per importare le voci specifiche da un file XML:

```
impex /xml:regcheck.xml /vuln:"Blaster Worm" /vulncat:"Registry
Vulnerabilities"
```

Esempio 2

Per importare un intero file XML:

```
impex /xml:regcheck.xml /im
```

Nota

L'eseguibile Impex può essere contenuto all'interno della cartella di installazione di GFI LanGuard.

Nota

Se gli elementi `<xmlfile>`, `<dbfile>`, `<name>`, `<category>` o `<value>` specificati contengono caratteri con spazi, l'intero valore deve essere racchiuso tra virgolette. Esempio:

- `<xmlfile>` contenente spazio = `"Definizioni controlli vulnerabilità.xml"`
- `<xmlfile>` senza spazio = `Definizionicontrollivulnerabilità.xml`

Nota

Nel caso in cui le vulnerabilità vengano importate in un'altra istanza installata di GFI LanGuard, l'installazione avrà lo stesso numero di build di quella da cui è stato esportato il database.

IMPORTANTE

Si consiglia vivamente di non utilizzare lo strumento **Impex** nel caso in cui l'applicazione GFI LanGuard (LanGuard.exe) o i profili di scansione LanGuard (scanprofiles.exe) siano in esecuzione.

14 Script Debugger

Gli script che identificano vulnerabilità personalizzate possono essere creati utilizzando qualsiasi linguaggio di script compatibile con VBScript. Per impostazione predefinita, GFI LanGuard viene fornito con un editor di script utile per creare script personalizzati.

Nell'elenco dei controlli supportati da GFI LanGuard è necessario includere nuovi controlli. Utilizzare la scheda Valutazione delle vulnerabilità per aggiungere nuovi controlli all'elenco predefinito dei controlli di vulnerabilità per ogni profilo di scansione. GFI LanGuard supporta anche l'esecuzione di script Python.

Argomenti del presente capitolo:

14.1 Creazione di script personalizzati tramite VBscript 237

14.2 Creazione di script personalizzati utilizzando il linguaggio di scripting Python 242

14.3 Modulo SSH 246

14.1 Creazione di script personalizzati tramite VBscript

GFI LanGuard supporta ed esegue script scritti nei linguaggi compatibili con VBscript. Utilizzare linguaggi compatibili con VBscript per creare script personalizzati che possono essere eseguiti sulle proprie destinazioni di rete.

Gli script dei controlli di sicurezza possono essere sviluppati utilizzando l'editor di script in dotazione con GFI LanGuard. Questo editor di script integrato comprende funzionalità di evidenziazione della sintassi nonché funzioni di debug utili durante lo sviluppo degli script. Aprire l'editor di script da **Start > Tutti i programmi > GFI LanGuard > LANGuard Script Debugger**.

Nota

1. Per ulteriori informazioni su come sviluppare script utilizzando l'editor di script integrato, consultare il file della guida **Documentazione scripting** incluso in **Start > Tutti i programmi > GFI LanGuard > Documentazione relativa a LanGuard Scripting**.

Nota

GFI non supporta richieste di assistenza relative a problemi che potrebbero verificarsi negli script personalizzati. È possibile pubblicare eventuali dubbi su GFI LanGuard sui forum disponibili alla pagina http://forums.gfi.com/. Attraverso questo forum è possibile condividere script, problemi e idee con altri utenti GFI LanGuard.

14.1.1 Aggiunta di un controllo di vulnerabilità che utilizza uno script VBScript (.vbs) personalizzato

Per creare nuovi controlli di vulnerabilità che utilizzano VBScript personalizzati, attenersi ai passaggi descritti nella presente sezione.

- Passaggio 1: Creare lo script
- Passaggio 2: Aggiungere nuovi controlli di vulnerabilità

» Passaggio 3: Verifica del controllo di vulnerabilità/script

Passaggio 1: Creare lo script

1. Avviare Script Debugger da **Start > Tutti i programmi > GFI LanGuard > LANguard Script Debugger**.

2. Andare in **File > Nuovo**.

3. Creare uno script. Per questo esempio, utilizzare il seguente codice di script fittizio.

```
Function Main
   echo "Script has run successfully"
   Main = true
End Function
```

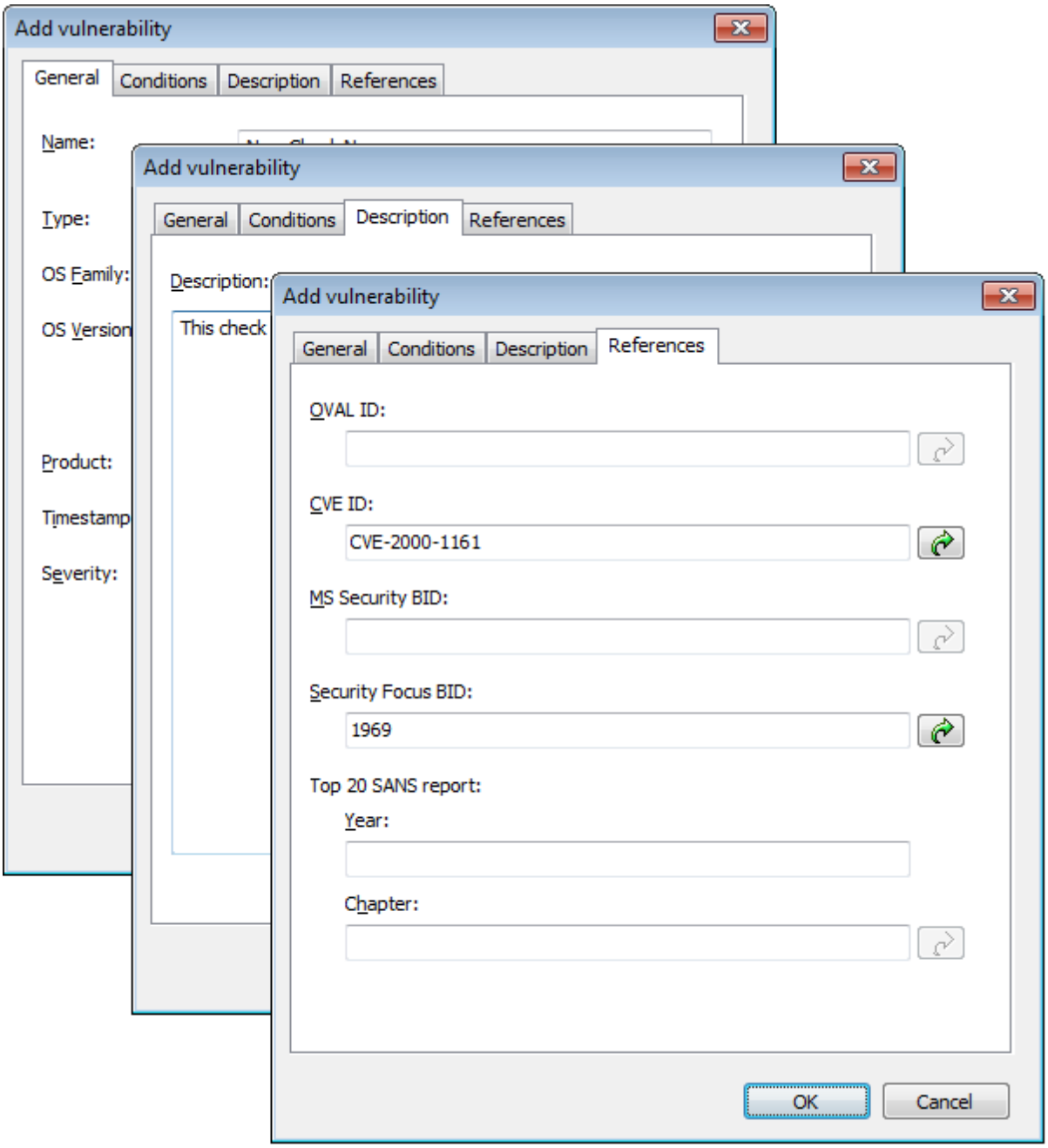
4. Salvare lo script in `<percorso della cartella di installazione LanGuard>\Data\Scripts\myscript.vbs`.

Passaggio 2: Aggiungere nuovi controlli di vulnerabilità

1. Avviare GFI LanGuard.

2. Fare clic sul pulsante GFI LanGuard e selezionare **Configurazione > Editor dei profili di scansione**. In alternativa, premere **CTRL + P** per avviare l'**Editor profili di scansione**.

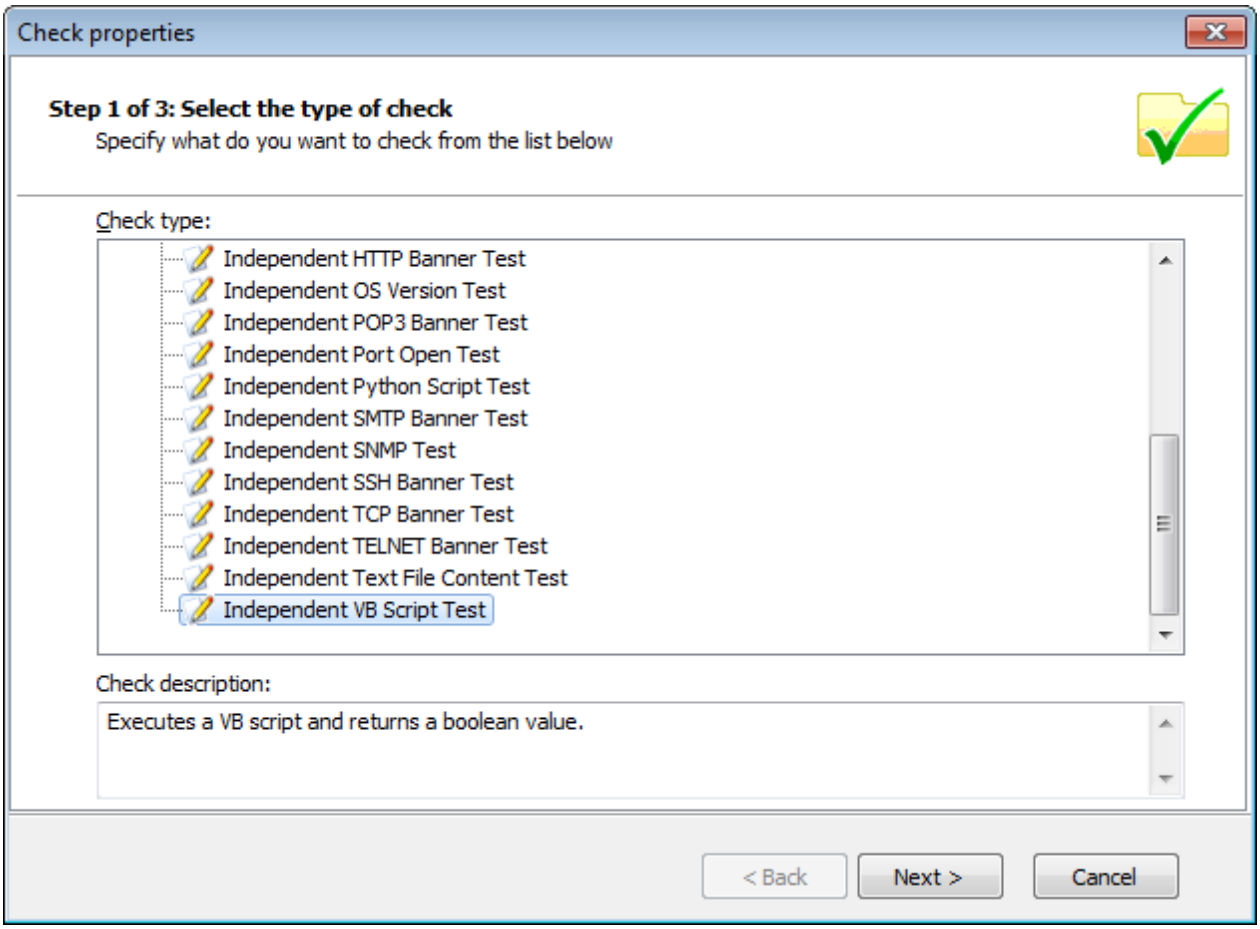
3. Nella nuova finestra aggiungere una nuova vulnerabilità facendo clic su **Aggiungi** sotto l'elenco dei controlli delle vulnerabilità.



Screenshot 156: Finestra di dialogo Aggiungi vulnerabilità

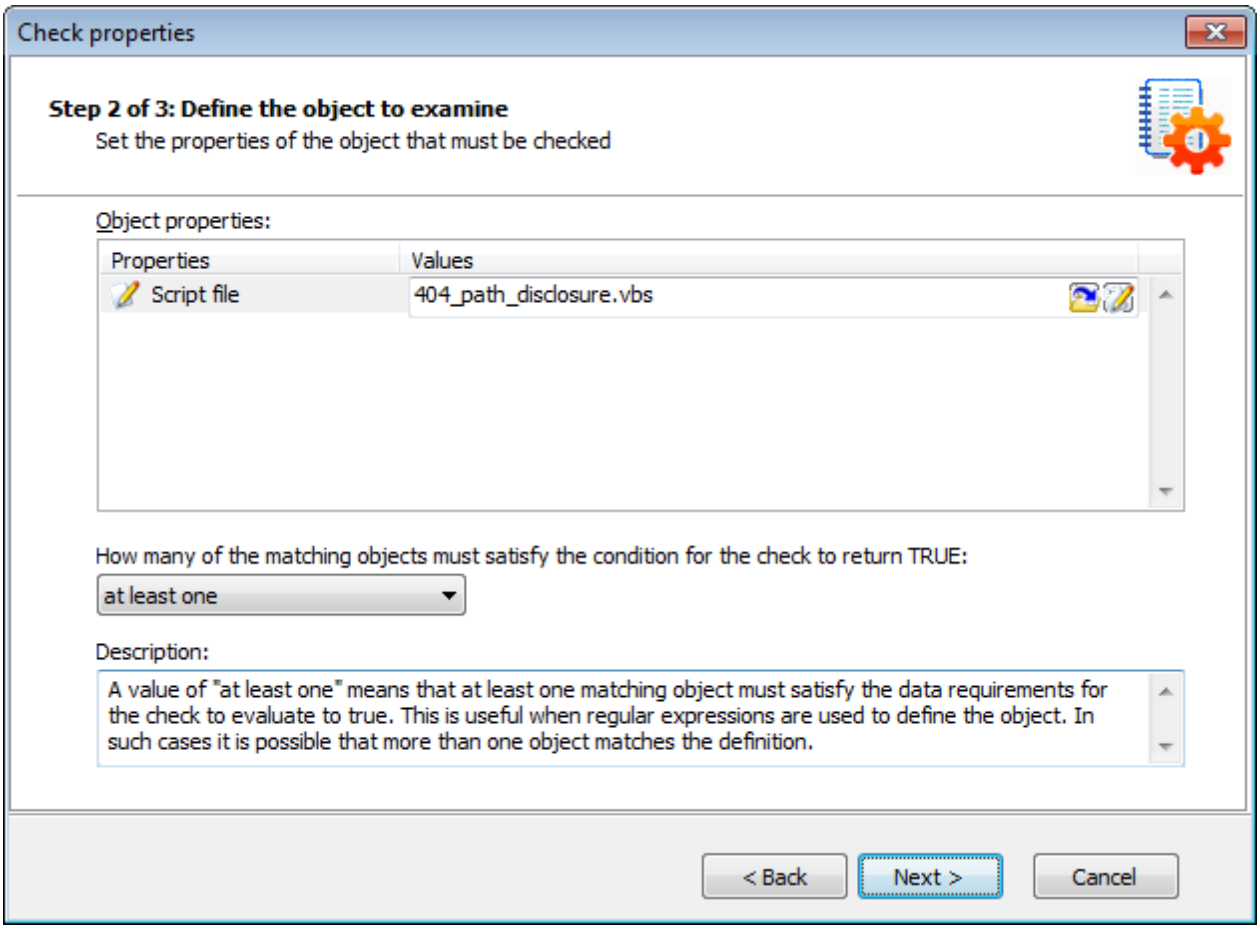
4. Nelle schede **Generale**, **Descrizione** e **Riferimenti** specificare i dettagli di base quali il nome della vulnerabilità, una breve descrizione, il livello di sicurezza e l'ID OVAL (se disponibile).

5. Fare clic sulla scheda **Condizioni** e fare clic sul pulsante **Aggiungi**. Verrà visualizzata la procedura guidata per il controllo delle proprietà.


Check properties
Step 1 of 3: Select the type of check
Specify what do you want to check from the list below
Check type:
Independent HTTP Banner Test
Independent OS Version Test
Independent POP3 Banner Test
Independent Port Open Test
Independent Python Script Test
Independent SMTP Banner Test
Independent SNMP Test
Independent SSH Banner Test
Independent TCP Banner Test
Independent TELNET Banner Test
Independent Text File Content Test
Independent VB Script Test
Check description:
Executes a VB script and returns a boolean value.
< Back
Next >
Cancel

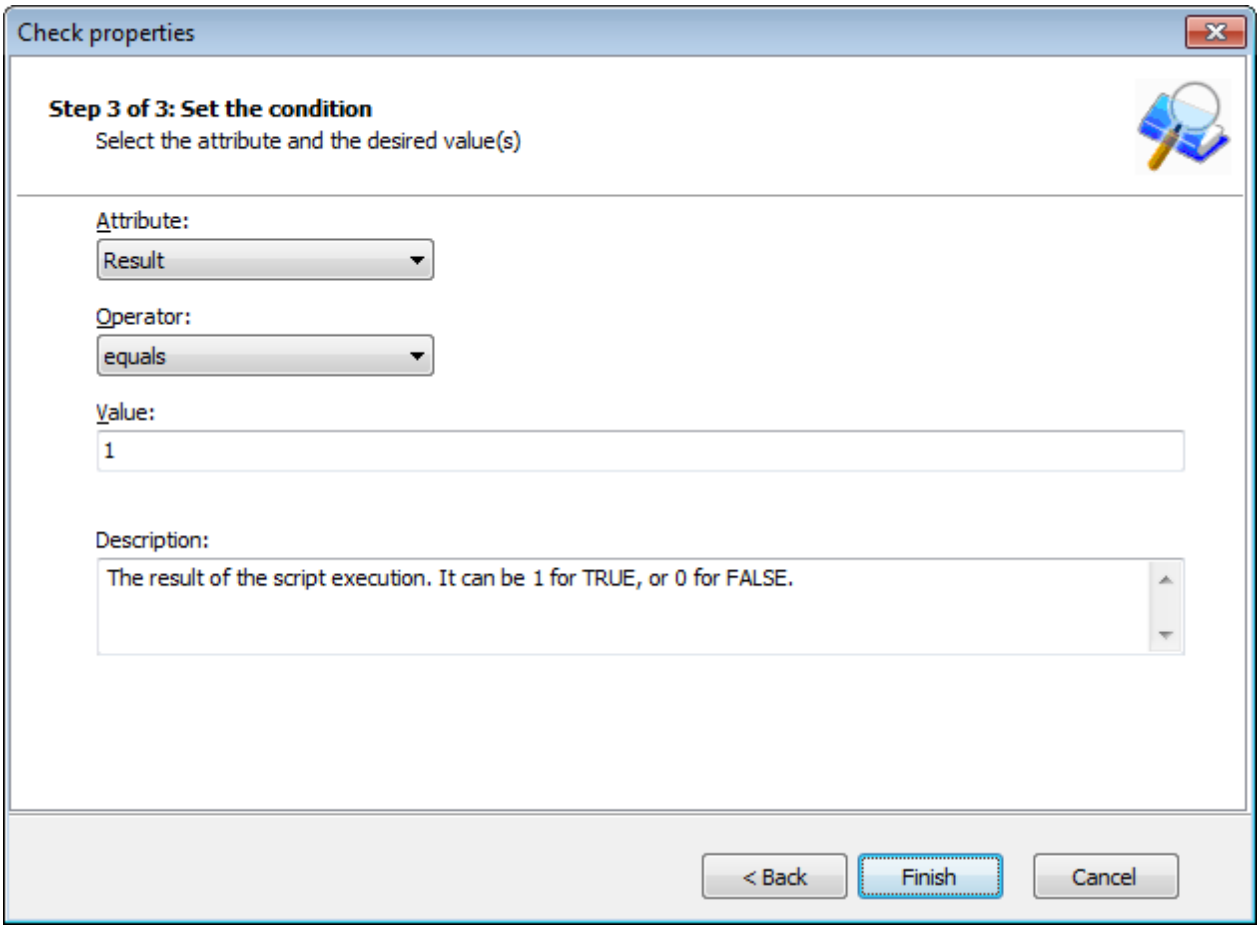
Screenshot 157: Aggiunta di controlli di vulnerabilità - Selezione del tipo di controllo

6. Selezionare il nodo **Controlli indipendenti > VBScript** e fare clic su **Avanti**.


Check properties
Step 2 of 3: Define the object to examine
Set the properties of the object that must be checked
Object properties:
Properties
Values
Script file
404_path_disclosure.vbs
How many of the matching objects must satisfy the condition for the check to return TRUE:
at least one
Description:
A value of "at least one" means that at least one matching object must satisfy the data requirements for the check to evaluate to true. This is useful when regular expressions are used to define the object. In such cases it is possible that more than one object matches the definition.
< Back
Next >
Cancel

Screenshot 158: Aggiunta di controlli di vulnerabilità - Selezione del file di script VB

7. Fare clic su **Scegli file** e selezionare il file VBscript personalizzato che verrà eseguito da questo controllo. Fare clic su **Avanti**.



Screenshot 159: Aggiunta di controlli di vulnerabilità - Definizione delle condizioni

8. Nella procedura guidata selezionare la configurazione delle condizioni appropriata per completare la selezione degli script. Fare clic su Fine per uscire dalla procedura guidata.

9. Fare clic su **OK** per salvare il nuovo controllo di vulnerabilità.

Passaggio 3: Verifica del controllo di vulnerabilità/script

Eseguire la scansione del computer host locale utilizzando il profilo di scansione in cui è stato aggiunto il nuovo controllo.

Dalla scheda **Scansione** > **Risultati**, verrà visualizzato un avviso nel nodo **Valutazione delle vulnerabilità** dei risultati della scansione.

14.2 Creazione di script personalizzati utilizzando il linguaggio di scripting Python

GFI LanGuard supporta anche un nuovo tipo di controllo delle vulnerabilità: il test script Python. Questo tipo di controllo è disponibile nell'ambito dei Controlli indipendenti.

Importante

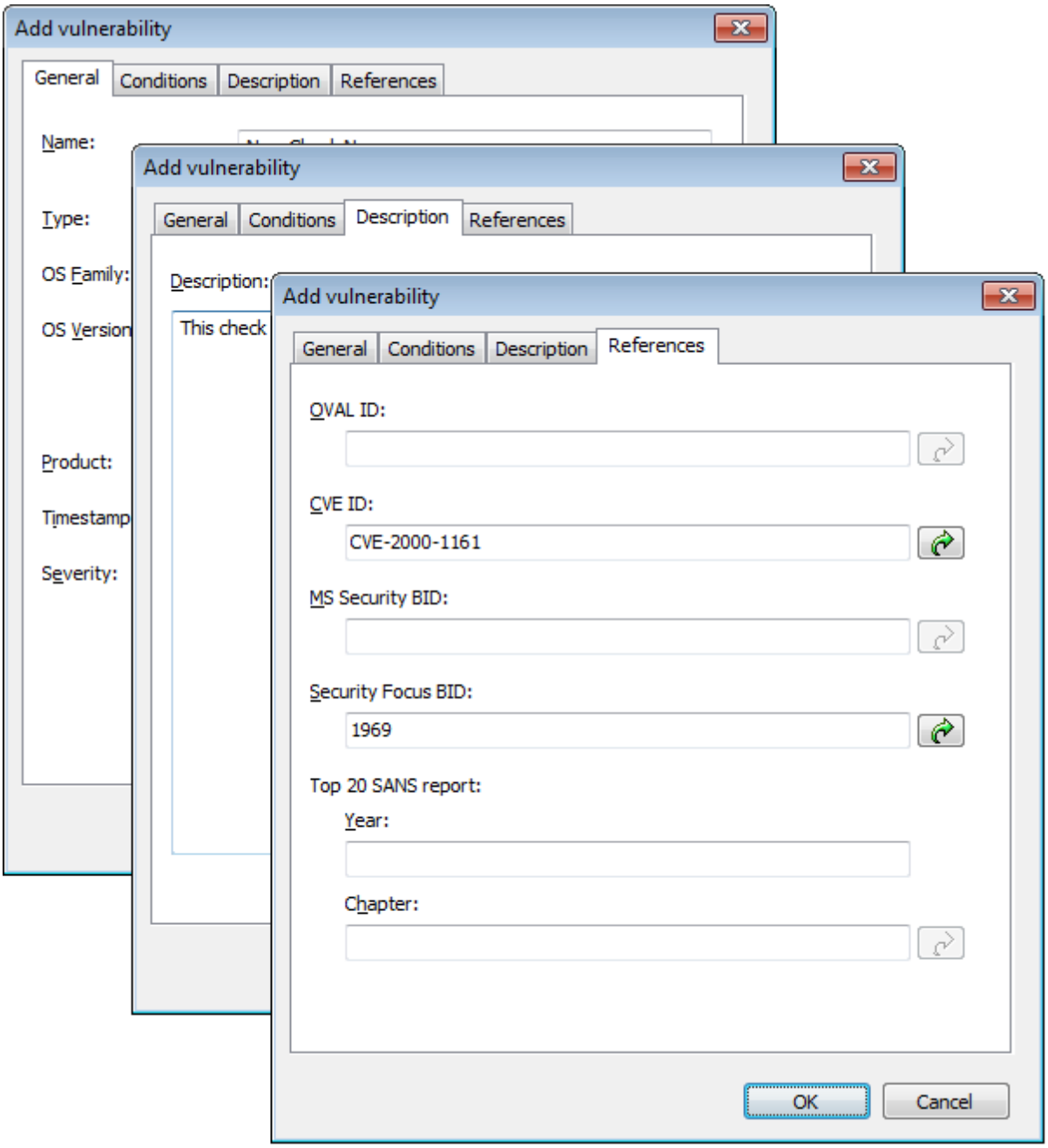
Per informazioni sullo scripting Python, fare riferimento alla documentazioni sugli script di GFI LanGuard da **Start > Tutti i programmi > GFI LanGuard 2012 > GFI LanGuard Documentazione script**.

Per aggiungere un nuovo controllo script python:

1. Avviare GFI LanGuard.

2. Fare clic sul pulsante GFI LanGuard e selezionare **Configurazione > Editor dei profili di scansione**. In alternativa, premere **CTRL + P** per avviare l'**Editor profili di scansione**.

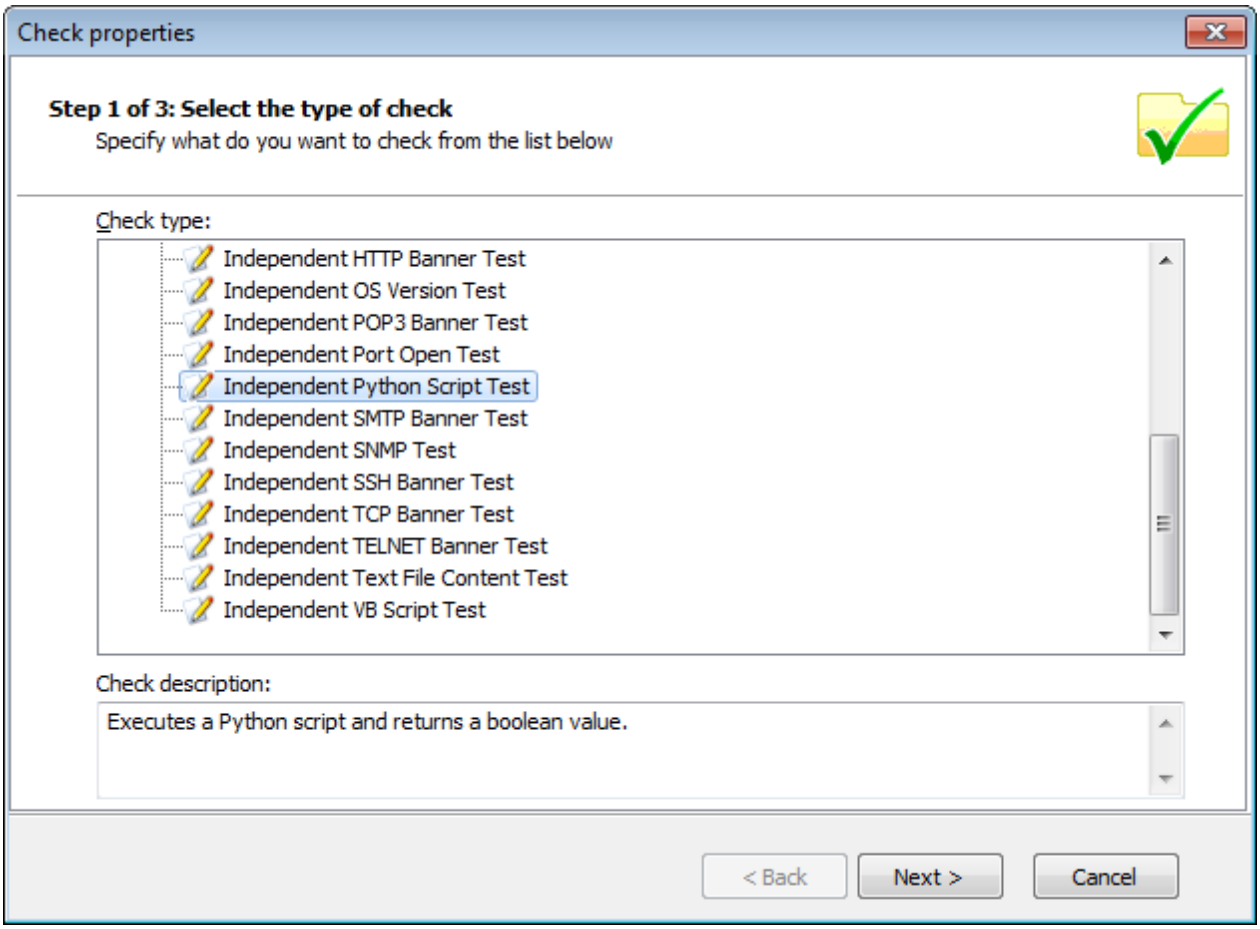
3. Nella nuova finestra aggiungere una nuova vulnerabilità facendo clic su **Aggiungi** sotto l'elenco dei controlli delle vulnerabilità.



Screenshot 160: Finestra di dialogo Aggiungi vulnerabilità

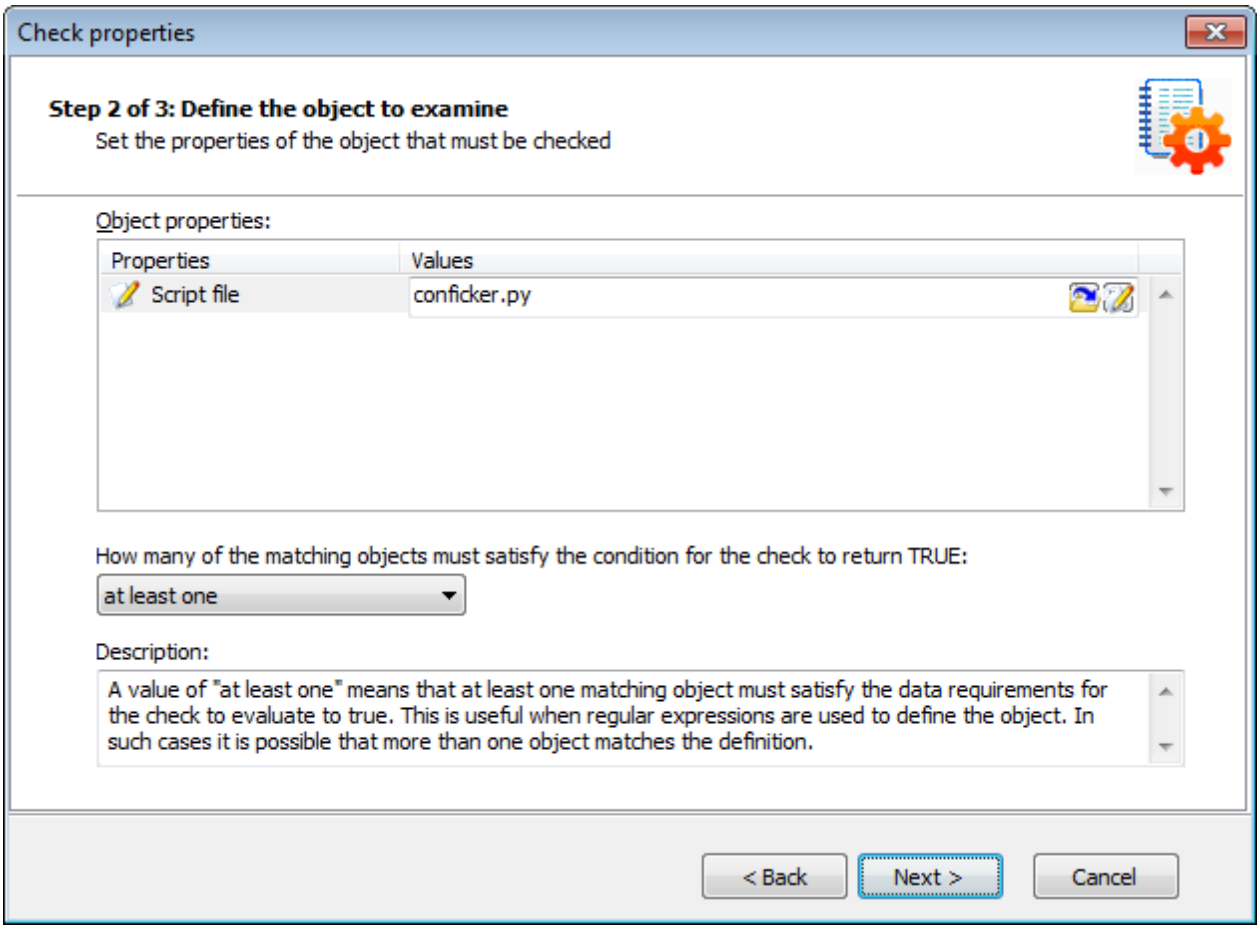
4. Nelle schede **Generale**, **Descrizione** e **Riferimenti** specificare i dettagli di base quali il nome della vulnerabilità, una breve descrizione, il livello di sicurezza e l'ID OVAL (se disponibile).

5. Fare clic sulla scheda **Condizioni** e fare clic sul pulsante **Aggiungi**. Verrà visualizzata la procedura guidata per il controllo delle proprietà.


Check properties
Step 1 of 3: Select the type of check
Specify what do you want to check from the list below
Check type:
Independent HTTP Banner Test
Independent OS Version Test
Independent POP3 Banner Test
Independent Port Open Test
Independent Python Script Test
Independent SMTP Banner Test
Independent SNMP Test
Independent SSH Banner Test
Independent TCP Banner Test
Independent TELNET Banner Test
Independent Text File Content Test
Independent VB Script Test
Check description:
Executes a Python script and returns a boolean value.
< Back
Next >
Cancel

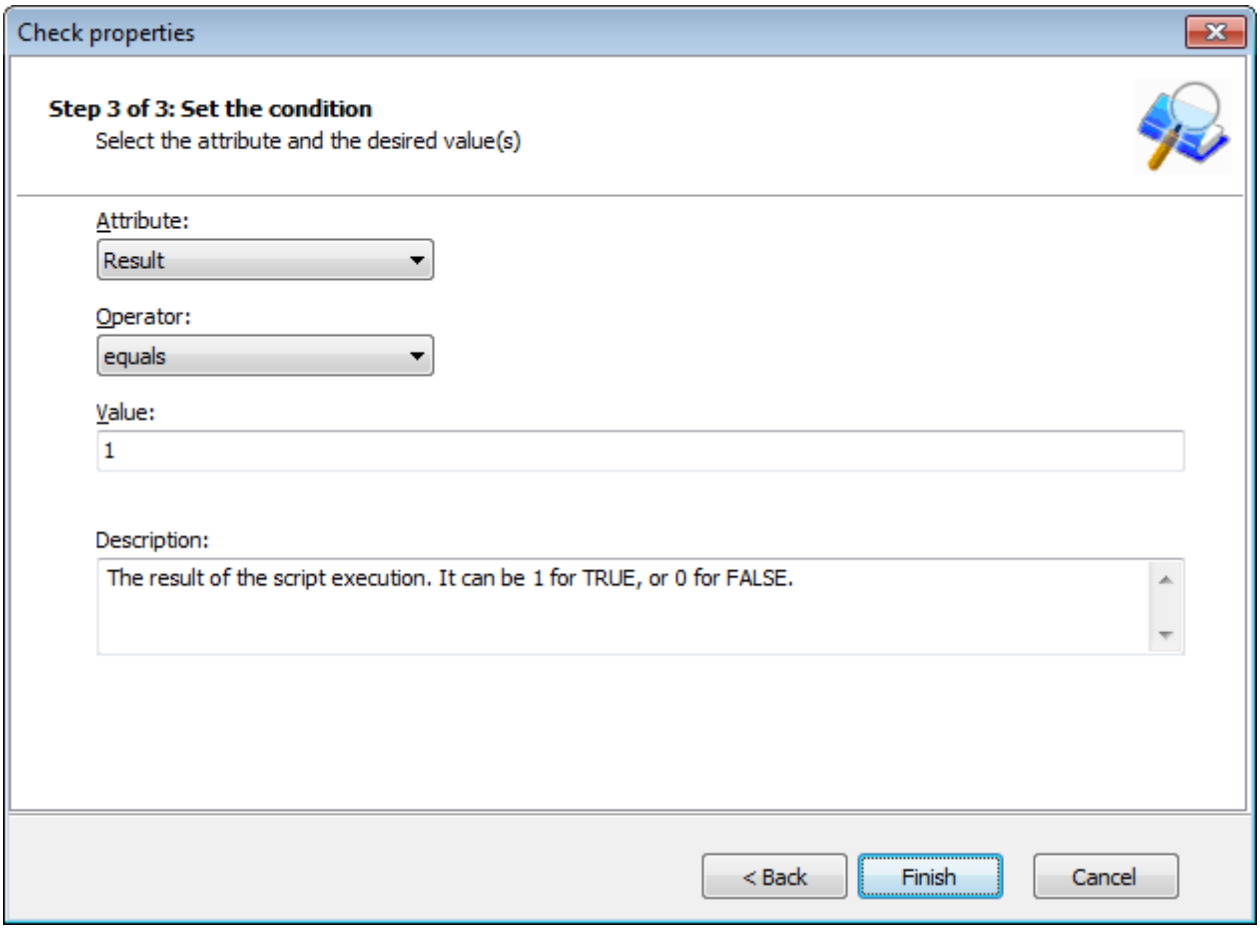
Screenshot 161: Aggiunta di controlli di vulnerabilità - Selezione del tipo di controllo

6. Selezionare il nodo **Controlli indipendenti > Test script python indipendente** e fare clic su **Avanti**.


Check properties
Step 2 of 3: Define the object to examine
Set the properties of the object that must be checked
Object properties:
Properties
Values
Script file
conficker.py
How many of the matching objects must satisfy the condition for the check to return TRUE:
at least one
Description:
A value of "at least one" means that at least one matching object must satisfy the data requirements for the check to evaluate to true. This is useful when regular expressions are used to define the object. In such cases it is possible that more than one object matches the definition.
< Back
Next >
Cancel

Screenshot 162: Aggiunta di controlli di vulnerabilità - Selezione del file di script python

7. Fare clic su **Scegli file** e selezionare il file di script Python personalizzato che verrà eseguito da questo controllo. Fare clic su **Avanti**.



Screenshot 163: Aggiunta di controlli di vulnerabilità - Definizione delle condizioni

8. Nella procedura guidata selezionare la configurazione delle condizioni appropriata per completare la selezione degli script. Fare clic su Fine per uscire dalla procedura guidata.

9. Fare clic su **OK** per salvare il nuovo controllo di vulnerabilità.

14.3 Modulo SSH

GFI LanGuard comprende un modulo SSH che gestisce l'esecuzione di script di vulnerabilità sui sistemi basati su Linux/UNIX.

Il modulo SSH determina il risultato dei controlli di vulnerabilità tramite i dati (testo) della console prodotti da uno script eseguito. Ciò significa che è possibile creare dei controlli personalizzati di vulnerabilità Linux/UNIX tramite qualsiasi metodo di scripting che è supportato dal sistema operativo del computer di destinazione.

14.3.1 Parole chiave

Il modulo SSH può eseguire script di scansione di sicurezza tramite la sua finestra terminale. Quando si lancia una scansione di sicurezza sui computer di destinazione basati su Linux/UNIX, gli script del controllo di vulnerabilità vengono copiati tramite una connessione SSH sul rispettivo computer di destinazione ed eseguiti in locale.

La connessione SSH viene stabilita utilizzando le credenziali di accesso (ossia nome utente e password/file di chiave privata SSH) specificate prima dell'avvio di una scansione di sicurezza.

Il modulo SSH può determinare lo stato di un controllo di vulnerabilità tramite parole chiave specifiche presenti nel testo dello script eseguito. Queste parole chiave vengono elaborate dal

modulo e interpretate come istruzioni per GFI LanGuard. Le parole chiave standard identificate dal modulo SSH comprendono le seguenti:

Table 90: Parole chiave di vulnerabilità

Parola chiave	Descrizione
TRUE: / FALSE	Queste stringhe indicano il risultato del controllo di vulnerabilità/script eseguito. Quando il modulo SSH rileva una parola chiave TRUE, significa che il controllo è stato completato correttamente; FALSE: indica che il controllo di vulnerabilità non è riuscito.
AddListItem	Questa stringa attiva una funzione interna che aggiunge i risultati al rapporto del controllo delle vulnerabilità (ossia i risultati della scansione). Questi risultati vengono visualizzati nella console di gestione GFI LanGuard al termine di una scansione. Questa stringa viene formattata come segue: `AddListItem([[[[parent node]]]],[[[[actual string]]]])`
[[[[nodo padre]]]]	Comprende il nome del nodo dei risultati della scansione nel quale verrà aggiunto il risultato.
[[[[stringa effettiva]]]]	Comprende il valore che verrà aggiunto nel nodo dei risultati della scansione. **Nota** Ogni controllo di vulnerabilità è correlato a un nodo dei risultati della scansione associato. Questo significa che i risultati 'AddListItem' sono inclusi per impostazioni predefinita in un nodo di vulnerabilità associato/predefinito. In tal modo, se il nodo superiore viene lasciato vuoto, la funzione aggiungerà la stringa specificata al nodo predefinito.
SetDescription	Questa stringa attiva una funzione interna che sovrascriverà la descrizione predefinita di un controllo di vulnerabilità con una nuova descrizione. Questa stringa viene formattata come segue: SetDescription([Nuova descrizione])
!!SCRIPT_ FINISHED!!	Questa stringa segna la fine di ogni esecuzione di script. Il modulo SSH continuerà a cercare questa stringa fino a quando non la troverà o fino a quando si verificherà un time-out. Se si verifica un time-out prima che venga generata la stringa "!!SCRIPT_FINISHED!!", il modulo SSH classificherà il rispettivo controllo di vulnerabilità come non riuscito. **Nota** È fondamentale che ogni script personalizzato emetta la stringa "!!SCRIPT_FINISHED!!" al completamento del processo di controllo.

14.3.2 Aggiunta di un controllo delle vulnerabilità che utilizza uno script di shell personalizzato

Nell'esempio riportato di seguito viene creato un controllo di vulnerabilità (per computer di destinazione basati su Linux) che utilizza uno script scritto in Bash. Il controllo di vulnerabilità in questo esempio tenterà di rilevare la presenza di un file fittizio denominato "test.file".

Passaggio 1: Creare lo script

1. Lanciare l'editor di file di testo preferito.

2. Creare un nuovo script utilizzando il seguente codice:

```
#!/bin/bash
if [ -e test.file ]
then
   echo "TRUE:"
else
   echo "FALSE:"
fi
echo "!!SCRIPT_FINISHED!!"
```

3. Salvare il file in `<percorso della cartella di installazione GFI LanGuard 2011>\..\Data\Scripts\myscript.sh`

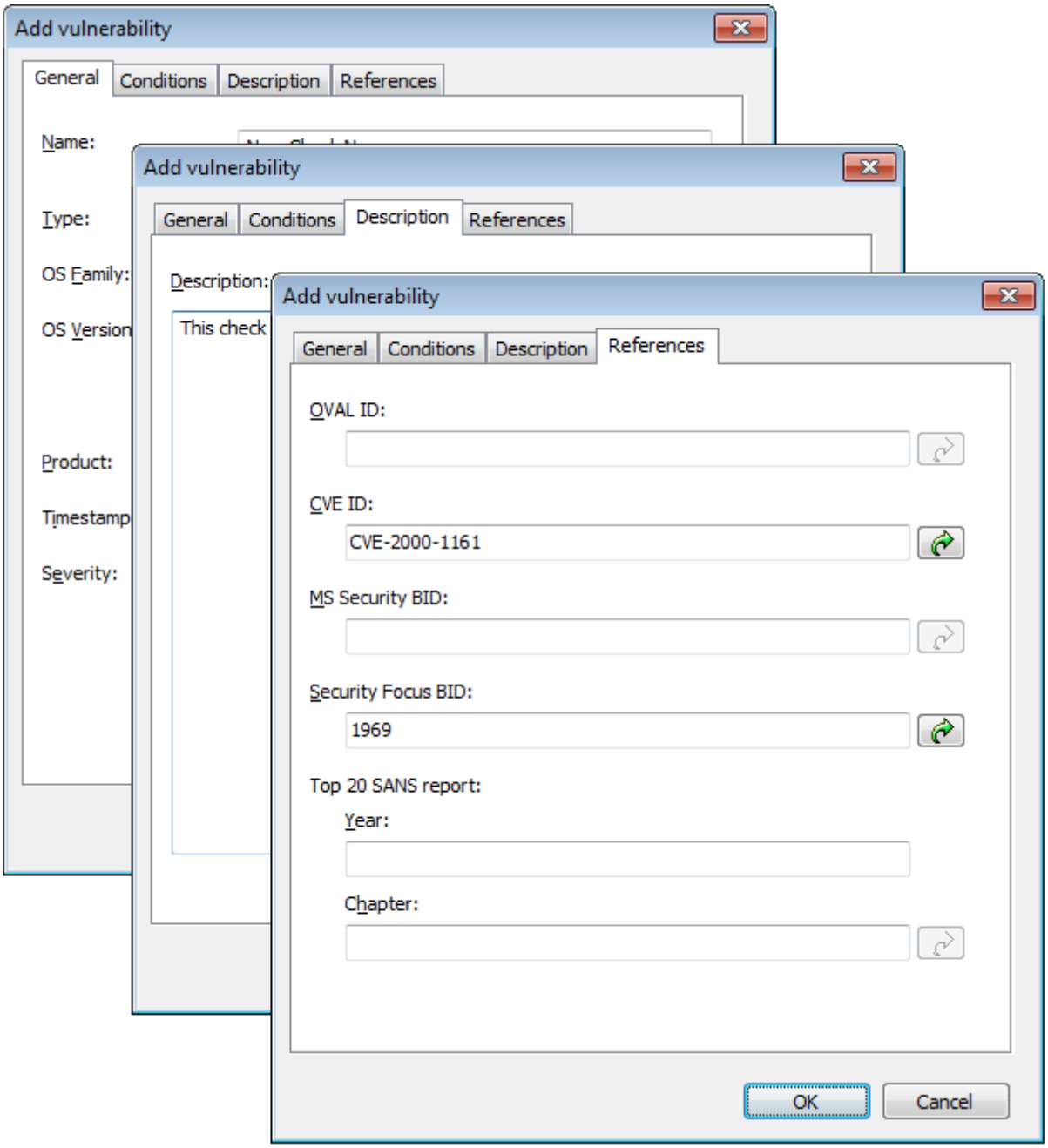
Passaggio 2: Aggiungere il nuovo controllo di vulnerabilità

1. Avviare GFI LanGuard.

2. Fare clic sul pulsante GFI LanGuard e selezionare **Configurazione > Editor dei profili di scansione**. In alternativa, premere **CTRL + P** per avviare l'**Editor profili di scansione**.

3. Dal riquadro centrale, selezionare la categoria in cui verrà inserito il nuovo controllo di vulnerabilità (ad esempio, Vulnerabilità di sicurezza di livello alto…).

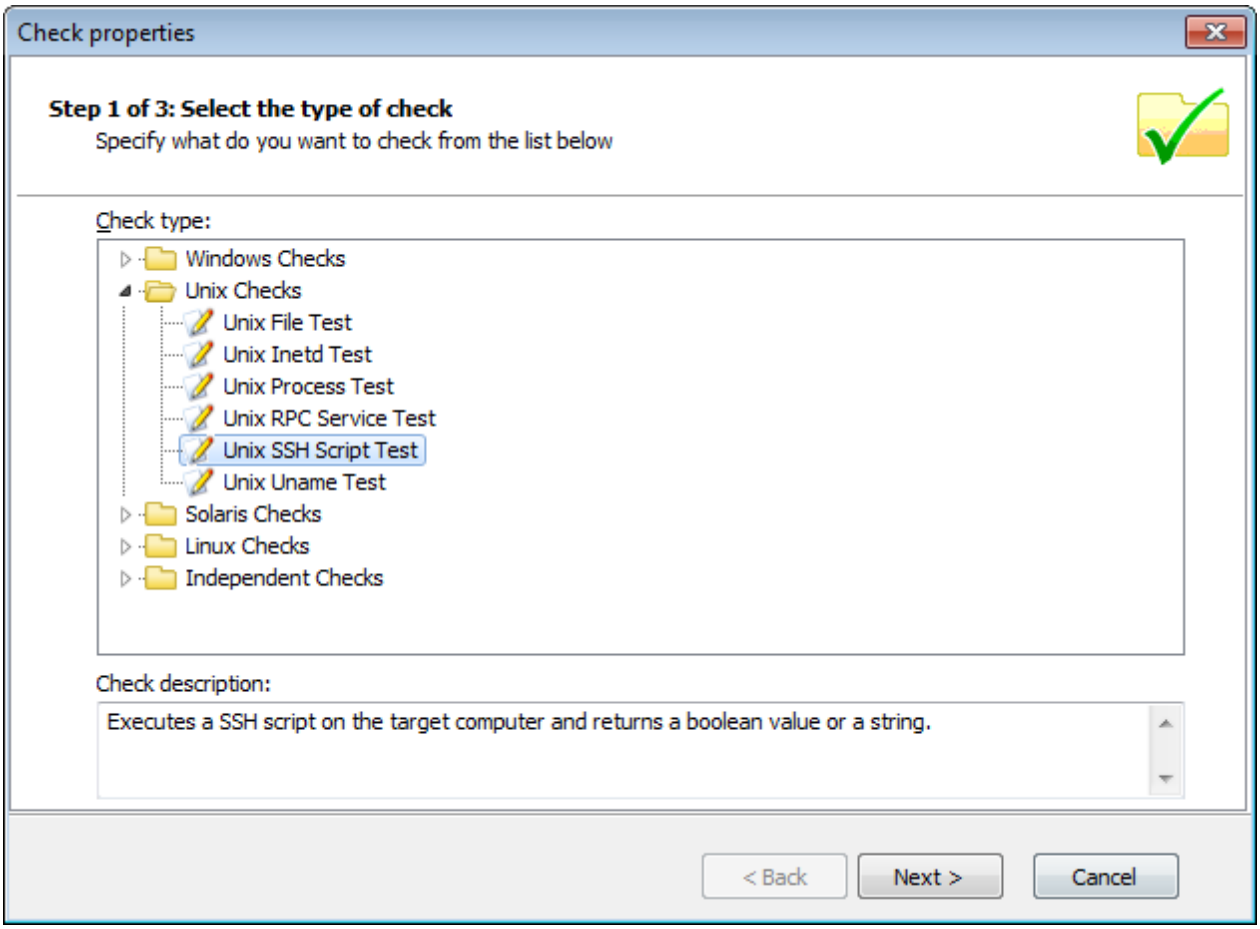
4. Nella nuova finestra, aggiungere una nuova vulnerabilità facendo clic su **Aggiungi** nel riquadro centrale.



Screenshot 164: Finestra di dialogo Aggiungi vulnerabilità

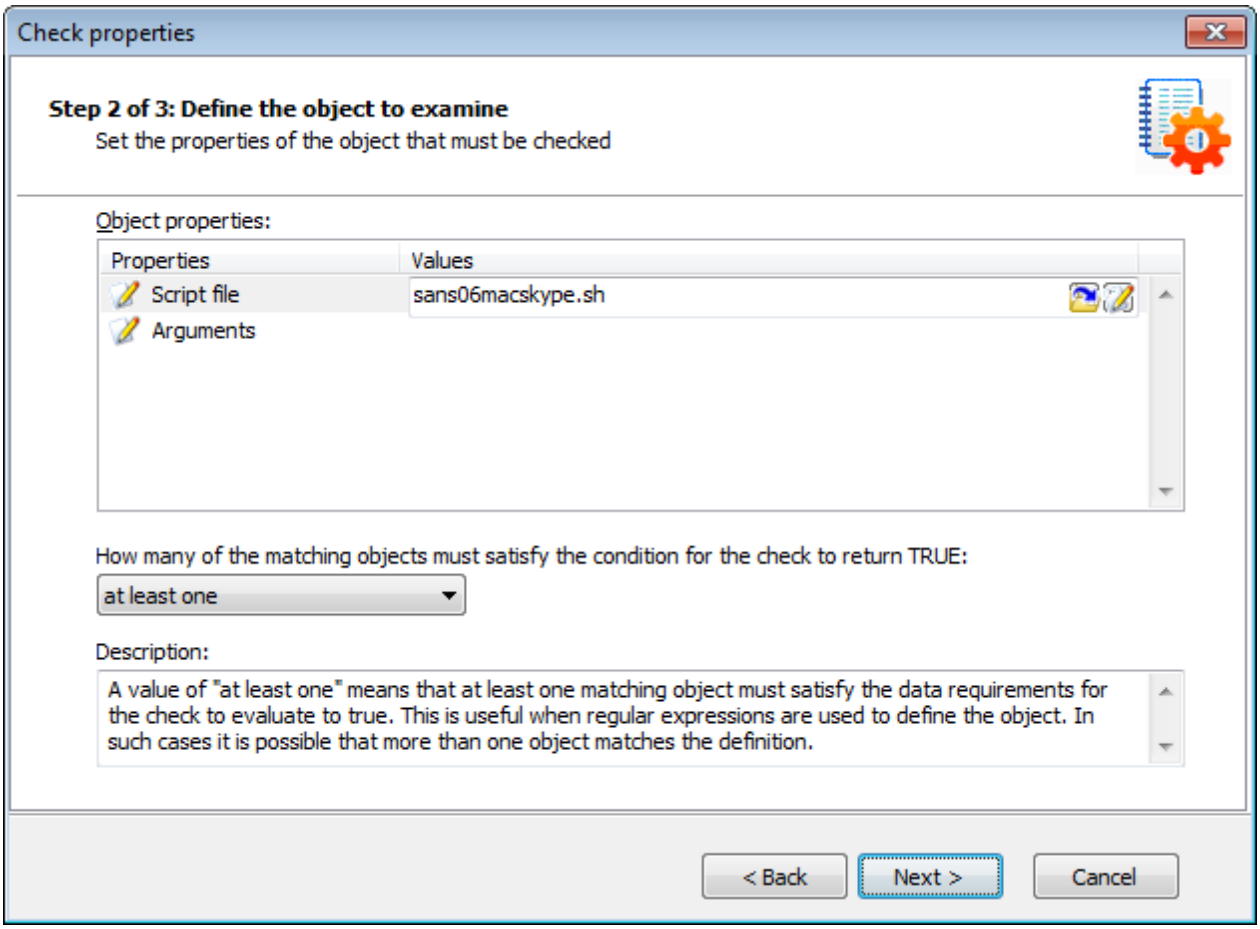
5. Nelle schede **Generale**, **Descrizione** e **Riferimento**, specificare i dettagli di base quali il nome della vulnerabilità, una breve descrizione, il livello di sicurezza e l'ID OVAL (se disponibile).

6. Scegliere la scheda **Condizioni** e fare clic sul pulsante **Aggiungi**. Verrà visualizzata la procedura guidata per il controllo delle proprietà.


Check properties
Step 1 of 3: Select the type of check
Specify what do you want to check from the list below
Check type:
Windows Checks
Unix Checks
Unix File Test
Unix Inetd Test
Unix Process Test
Unix RPC Service Test
Unix SSH Script Test
Unix Uname Test
Solaris Checks
Linux Checks
Independent Checks
Check description:
Executes a SSH script on the target computer and returns a boolean value or a string.
< Back
Next >
Cancel

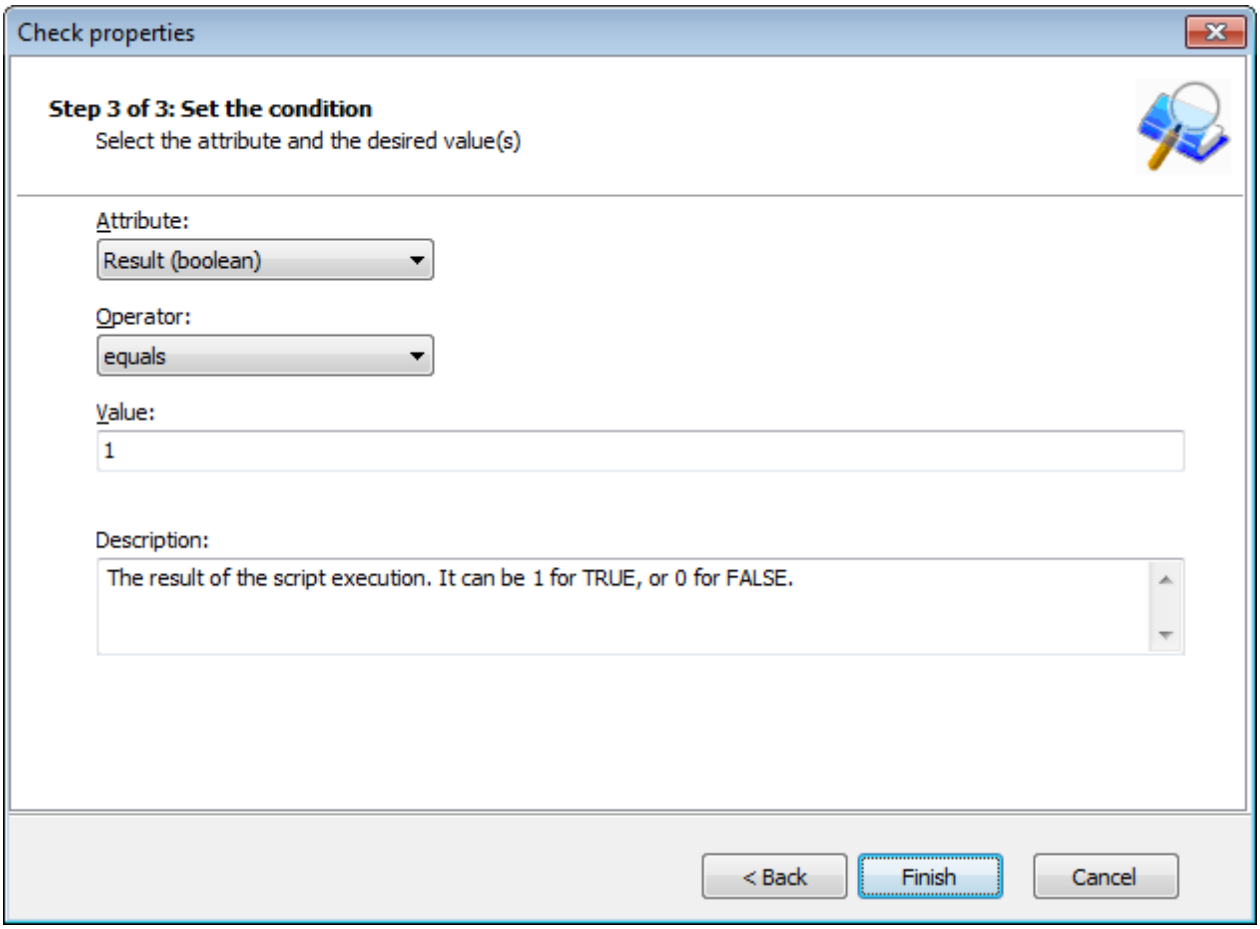
Screenshot 165: Aggiunta di controlli di vulnerabilità - Selezione del tipo di controllo

7. Selezionare il nodo **Controlli Unix > Test script SSH** e fare clic sul pulsante Avanti per continuare la configurazione.


Check properties
Step 2 of 3: Define the object to examine
Set the properties of the object that must be checked
Object properties:
Properties
Values
Script file
sans06macskype.sh
Arguments
How many of the matching objects must satisfy the condition for the check to return TRUE:
at least one
Description:
A value of "at least one" means that at least one matching object must satisfy the data requirements for the check to evaluate to true. This is useful when regular expressions are used to define the object. In such cases it is possible that more than one object matches the definition.
< Back
Next >
Cancel

Screenshot 166: Aggiunta di controlli di vulnerabilità - Selezione del file SSH

8. Fare clic su **Scegli file** e selezionare il file SSH script personalizzato che verrà eseguito durante questo controllo. Fare clic su **Avanti** per continuare.



Screenshot 167: Aggiunta di controlli di vulnerabilità - Definizione delle condizioni

9. Nella procedura guidata, selezionare la configurazione delle condizioni appropriata per completare la selezione degli script. Fare clic su Fine per uscire dalla procedura guidata.

10. Fare clic su **OK** per salvare il nuovo controllo di vulnerabilità.

Passaggio 3: Verifica del controllo di vulnerabilità/script utilizzato nell'esempio

Eseguire la scansione del computer host locale utilizzando il profilo di scansione in cui è stato aggiunto il nuovo controllo.

1. Accedere a un computer di destinazione Linux e creare un file denominato "test.file". Qualora trovasse un file denominato "test.file", questo controllo genererà un avviso di vulnerabilità.

2. Lanciare una scansione sul computer di destinazione Linux in cui è stato creato il file.

3. Controllare i risultati della scansione.

15 Funzioni varie

Il capitolo contiene informazioni sulla configurazione del NetBIOS nei computer e sulla modalità di disinstallazione di GFI LanGuard.

Argomenti del presente capitolo:

15.1 Configurazione di NetBIOS 252
15.2 Disinstallazione GFI LanGuard 253

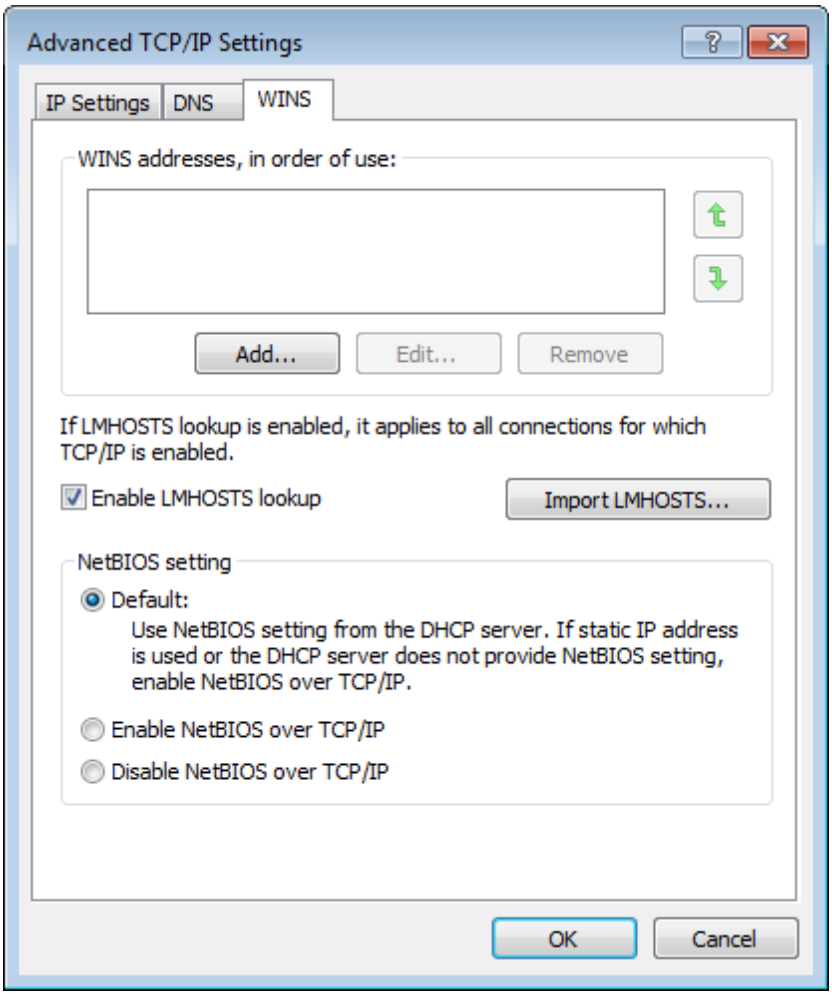
15.1 Configurazione di NetBIOS

Per verificare se le destinazioni di scansione utilizzano NetBIOS:

1. Selezionare **Pannello di controllo > Rete e Internet >Centro connessioni di rete e condivisione > Modifica impostazioni scheda.**

> **Nota**
> In Windows® XP fare clic su **Pannello di controllo > Connessioni di rete**.

2. Fare clic con il pulsante destro del mouse su **Connessione alla rete locale** e selezionare **Proprietà**.
3. Fare clic su **Protocollo Internet (TCP/IP)** e selezionare **Proprietà**.
4. Fare clic su **Avanzate > WINS**.


Advanced TCP/IP Settings
IP Settings
DNS
WINS
WINS addresses, in order of use:
Add...
Edit...
Remove
If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.
Enable LMHOSTS lookup
Import LMHOSTS...
NetBIOS setting
Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.
Enable NetBIOS over TCP/IP
Disable NetBIOS over TCP/IP
OK
Cancel

Screenshot 168: Finestra di dialogo delle proprietà della connessione alla rete locale: scheda WINS

5. Dall'area **Impostazione NetBIOS** assicurarsi che siano selezionate le opzioni **Predefinite** o **Abilita NetBIOS su TCP/IP**.

6. Fare clic su **OK** e chiudere le finestre di dialogo delle **proprietà della rete locale**.

Nota

Se si utilizza un indirizzo IP statico o se il server DHCP non fornisce l'impostazione NetBIOS, selezionare l'opzione Abilita NetBIOS su TCP/IP.

15.2 Disinstallazione GFI LanGuard

Per disinstallare GFI LanGuard:

1. Fare clic su **Start > Pannello di controllo > Installazione applicazioni**.

2. Selezionare GFI LanGuard dall'elenco e fare clic su **Rimuovi**.

3. Nella procedura guidata di disinstallazione, fare clic su **Avanti**.

4. Scegliere i file di dati di configurazione da rimuovere con la disinstallazione, quindi fare clic su **Avanti**.

5. Al termine, fare clic su **Fine**.

16 Risoluzione dei problemi e supporto

In questo capitolo viene spiegato come risolvere i problemi che si possono verificare durante l'utilizzo di GFI LanGuard. Questi problemi possono essere risolti utilizzando i contenuti di questa **Guida dell'amministratore**. In caso di problemi irrisolti anche dopo aver esaminato il manuale, controllare se il problema è incluso nell'elenco che segue.

Per ulteriori informazioni in merito alla risoluzione dei problemi comuni e per contattare il nostro team di supporto, fare riferimento alle seguenti sezioni.

Argomenti del presente capitolo:

16.1 Risoluzione di problemi comuni 254
16.2 Utilizzo della risoluzione guidata dei problemi 256
16.3 GFI SkyNet 258
16.4 Forum Web 258
16.5 Richiesta di supporto tecnico 258

16.1 Risoluzione di problemi comuni

La tabella in basso fornisce le soluzione ai problemi più comuni che possono essere riscontrati quando si utilizza GFI LanGuard:

Table 91: GFI LanGuard Problemi comuni

Problema rilevato	Soluzione/Descrizione
Errore di connessione al database viene riscontrato quando si cerca di configurare il database back-end.	**Descrizione** Questo problema può verificarsi in presenza delle seguenti due condizioni: 1. GFI LanGuard è installato su Windows 2000 SP4 con MDAC 2.5 SP 3 2. Il database back-end è SQL Server®, dove il nome istanza database è diverso dal nome del computer SQL Server®. **Soluzione** Installare **Microsoft® Data Access Components** (MDAC 2.6 o versioni successive) sul computer GFI LanGuard e riprovare. È possibile scaricare MDAC dall'indirizzo: http://go.gfi.com/?pageid=download_mdac
La struttura del database non è corretta. Procedere all'eliminazione e ricreazione del data base? Questo avviso viene riscontrato quando si cerca di configurare il database back-end.	**Descrizione** Il problema si verifica quando la struttura del database è danneggiata. Oppure Il database restituisce un timeout perché non è possibile stabilire la connessione. **Soluzione** Quando si riceve questo messaggio: Verificare che tutte le credenziali SQL siano corrette e che non vi siano problemi di connettività tra il computer dove si trova GFI LanGuard e il SQL Server. È importante notare che la selezione di OK comporterà la perdita di tutte le scansioni salvate.

Problema rilevato	Soluzione/Descrizione
Durante la configurazione di un database SQL, quando si tenta di accedere alla scheda Modifica database si riceve il messaggio Impossibile connettersi al data base.	**Descrizione** Questo problema può verificarsi in presenza delle seguenti due condizioni: » GFI LanGuard è installato su Windows 2000 SP4 con MDAC 2.5 SP 3. » Il database back-end è SQL Server®, dove il nome istanza database è diverso dal nome del computer SQL Server®. **Soluzione** Installare Microsoft® Data Access Components (MDAC 2.6 o versioni successive) sul computer GFI LanGuard e riprovare. **Nota** È possibile scaricare MDAC dall'indirizzo: http://go.gfi.com/?pageid=download_mdac
Risultati incompleti ed errori durante la scansione di computer remoti	**Descrizione** È possibile riscontrare errori simili ai seguenti: » Impossibile aprire chiave di test per il registro remoto. » La scansione viene interrotta. » Accesso negato » Impossibile connettersi al server SMB remoto. Questi errori possono essere riscontrati per i seguenti motivi: » Il computer remoto dispone di un account simile a quello utilizzato da GFI LanGuard per accedere come amministratore. » L'account utente utilizzato da GFI LanGuard non dispone di privilegi amministrativi. **Soluzione** Per risolvere questo problema eseguire una delle seguenti operazioni: » Accedere al computer dove si trova GFI LanGuard e configurare GFI LanGuard affinché utilizzi un account amministratore di un dominio alternativo. » Eliminare l'account utente locale dal computer remoto. » Avviare l'eseguibile di GFI LanGuard con il comando "Esegui come" di un account amministratore di dominio. **Nota** Per maggiori informazioni, consultare: http://go.gfi.com/?pageid=LAN_ProbScanningRM
Impossibile eseguire gli aggiornamenti del programma GFI LanGuard	**Descrizione** Gli aggiornamenti non funzioneranno se il computer dove è presente GFI LanGuard non dispone di connessione diretta a Internet. **Soluzione** Per risolvere questo problema eseguire una delle seguenti operazioni: » Configurare il computer GFI LanGuard affinché disponga di accesso diretto a Internet. » Installare un'altra istanza di GFI LanGuard su un computer con accesso a Internet e configurare GFI LanGuard per il controllo degli aggiornamenti dalla nuova installazione. **Nota** Per ulteriori informazioni, fare riferimento a http://go.gfi.com/?pageid=LAN_CheckAltUpdates

Problema rilevato	Soluzione/Descrizione
Il firewall installato su GFI LanGuard blocca la connessione ai computer di destinazione	**Descrizione** La scansione potrebbe rallentare o essere bloccata se il firewall è installato sul computer dove è presente GFI LanGuard. **Soluzione** Configurare il firewall per consentire ai seguenti componenti le connessioni in uscita: » <..\Program Files\GFI\LanGuard>*.exe » <..\Program Files\GFI\LanGuard Agent>*.exe **Nota** Per maggiori informazioni, consultare: http://go.gfi.com/?pageid=LAN_SetBestPerformance
GFI LanGuard non riesce a recuperare i computer del gruppo di lavoro quando si utilizza la funzione Enumera computer	**Descrizione** GFI LanGuard utilizza il meccanismo di Windows per recuperare i computer da un gruppo di lavoro. Grazie a questo meccanismo, un computer Master Browser crea e archivia un elenco di tutti i computer. In alcuni casi, il ruolo di Master Browser può non riuscire, di conseguenza GFI LanGuard non è in grado di recuperare le informazioni dei computer. **Nota** Per risolvere questo problema, fare riferimento a http://go.gfi.com/?pageid=LAN_CannotEnumerate
GFI LanGuard ha trovato delle porte aperte che un altro scanner delle porte ha rilevato come chiuse	**Descrizione** GFI LanGuard utilizza un approccio diverso rispetto ad altri scanner delle porte per il rilevamento delle porte aperte. **Soluzione** Per visualizzare lo stato di una porta e determinare se è chiusa o aperta: 1. Fare clic su **Start > Tutti i programmi > Accessori > Prompt dei comandi**. 2. Digitare `netstat -an` e premere **Invio**. 3. L'elenco generato visualizza tutte le connessioni attive del computer.

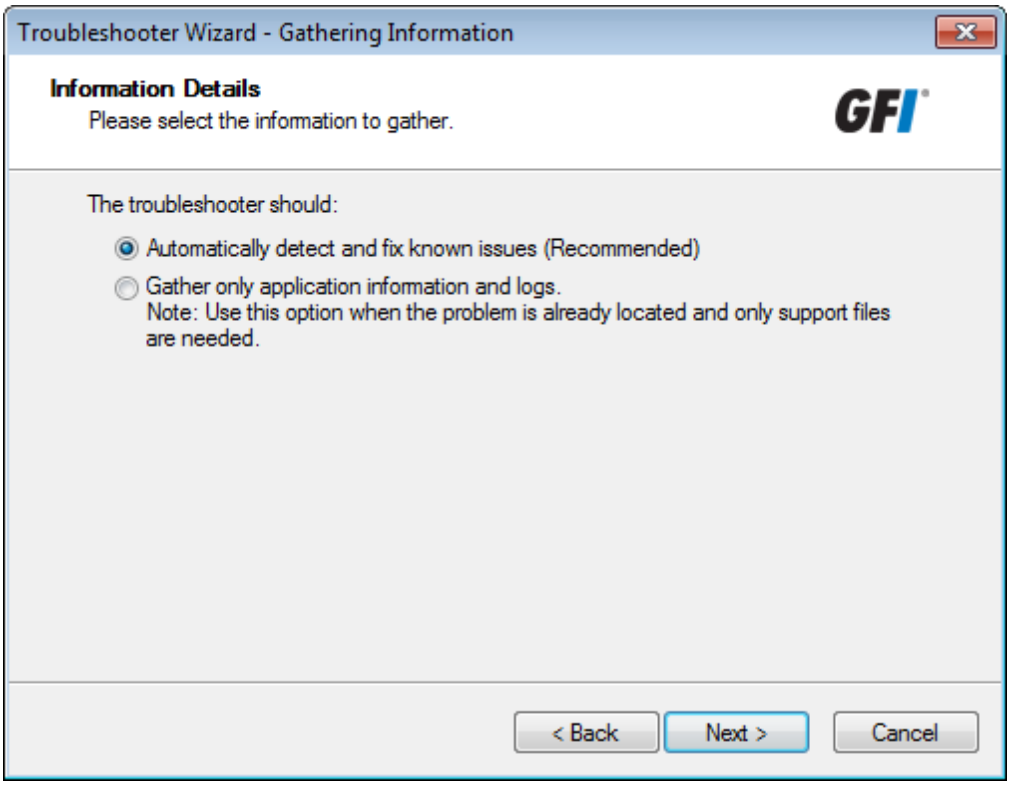
16.2 Utilizzo della risoluzione guidata dei problemi

La risoluzione guidata dei problemi GFI LanGuard è uno strumento concepito per assistere gli utenti quando si verificano problemi tecnici relativi all'utilizzo di GFI LanGuard. Questa procedura guidata consente di rilevare e correggere automaticamente problemi comuni nonché raccogliere le informazioni e i registri da inviare al team di supporto tecnico.

Per utilizzare la risoluzione guidata dei problemi:

1. Avviare la risoluzione guidata dei problemi da **Start > Tutti i programmi > GFI LanGuard 2012 > GFI LanGuard 2012 Troubleshooter**.

2. Fare clic su **Avanti** nella pagina di introduzione.


Troubleshooter Wizard - Gathering Information
Information Details
Please select the information to gather.
GFI
The troubleshooter should:
Automatically detect and fix known issues (Recommended)
Gather only application information and logs.
Note: Use this option when the problem is already located and only support files are needed.
< Back
Next >
Cancel

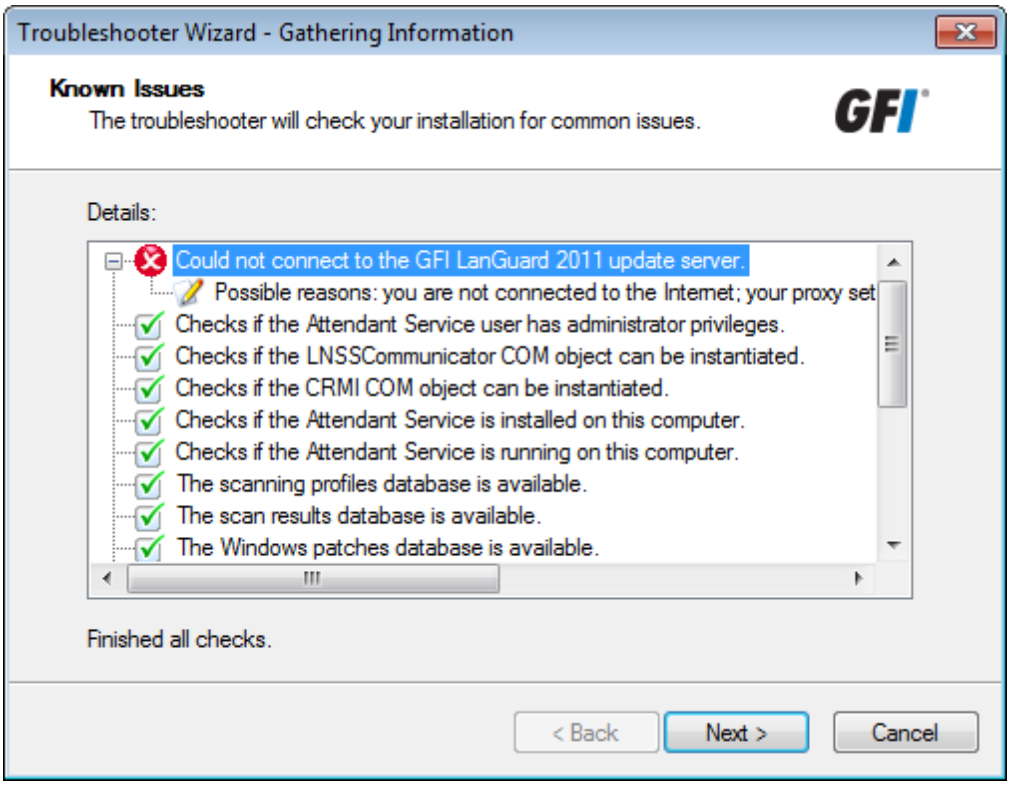
Screenshot 169: Risoluzione guidata dei problemi - Dettagli sulle informazioni

3. Nella pagina Dettagli sulle informazioni, selezionare una delle seguenti opzioni descritte di seguito:

Table 92: Opzioni di raccolta informazioni

Opzione	Descrizione
Rileva e risolvi automaticamente i problemi noti	(Consigliato) Configurare GFI LanGuard per la rilevazione e risoluzione automatica dei problemi.
Raccogli solo le informazioni e i registri delle applicazioni	Raccoglie registri da inviare all'assistenza GFI.

4. Per continuare, fare clic su **Avanti**.


Troubleshooter Wizard - Gathering Information
Known Issues
The troubleshooter will check your installation for common issues.
GFI
Details:
Could not connect to the GFI LanGuard 2011 update server.
Possible reasons: you are not connected to the Internet; your proxy set
Checks if the Attendant Service user has administrator privileges.
Checks if the LNSSCommunicator COM object can be instantiated.
Checks if the CRMI COM object can be instantiated.
Checks if the Attendant Service is installed on this computer.
Checks if the Attendant Service is running on this computer.
The scanning profiles database is available.
The scan results database is available.
The Windows patches database is available.
Finished all checks.
< Back
Next >
Cancel

Screenshot 170: Risoluzione guidata dei problemi - Raccolta delle informazioni sui problemi noti

5. La risoluzione guidata dei problemi recupererà tutte le informazioni necessarie per risolvere i problemi comuni. Per continuare, fare clic su **Avanti**.

6. Il programma di risoluzione dei problemi risolverà qualsiasi problema noto che si presenterà. Selezionare **Sì** se il problema è stato risolto o **No** se il problema non è stato risolto per cercare informazioni nella Knowledge base di GFI.

16.3 GFI SkyNet

GFI cura la gestione di una Knowledge Base completa contenente le risposte ai problemi più comuni. GFI SkyNet contiene sempre l'elenco più aggiornato delle domande e delle patch fornite dal supporto tecnico. Se le informazioni contenute nella presente guida non risolvono i problemi, fare riferimento a GFI SkyNet all'indirizzo: http://kb.gfi.com/.

16.4 Forum Web

L'assistenza tecnica tra utenti è disponibile sul forum Web di GFI. Il forum Web è disponibile all'indirizzo: http://forums.gfi.com

16.5 Richiesta di supporto tecnico

Se nessuna delle risorse precedenti ha permesso di risolvere i problemi, contattare il personale di assistenza tecnica di GFI compilando il modulo di richiesta online o telefonando.

- **Online**: Compilare il modulo di richiesta di supporto e seguire rigorosamente le istruzioni indicate nella pagina per inviare la richiesta: http://support.gfi.com/supportrequestform.asp
- **Telefono**: Per ottenere il numero telefonico corretto dell'assistenza tecnica della regione competente, visitare il sito: http://www.gfi.com/company/contact.htm

Nota

Prima di contattare l'assistenza tecnica, accertarsi di avere a disposizione l'ID cliente. L'ID cliente è il numero dell'account cliente online assegnato alla prima registrazione delle chiavi di licenza nell'Area clienti GFI alla pagina http://customers.gfi.com.

Il team risponderà alla richiesta entro 24 ore al massimo, a seconda del fuso orario.

Documentazione

Se questo manuale non soddisfa le attese o si ritiene che possa in qualche modo essere migliorato, inviare un messaggio di posta elettronica a: documentation@gfi.com.

17 Appendice 1 - Dati elaborati

In fase di controllo reti, GFI LanGuard enumera ed elabora le informazioni seguenti. Si tratta di informazioni che vengono raccolte dalle destinazioni di scansione utilizzando le porte e i protocolli descritti nelle sezioni in basso.

Argomenti del presente capitolo:

17.1 Stato dell'applicazione di patch al sistema 260
17.2 Porte 261
17.3 Hardware 261
17.4 Software 263
17.5 Informazioni di sistema 266

17.1 Stato dell'applicazione di patch al sistema

Dati	Descrizione	Porte	Protocollo
Service pack e aggiornamenti cumulativi mancanti	Rileva i service pack mancanti Microsoft® e non Microsoft®.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » Agente Windows Update
Aggiornamenti di sicurezza mancanti	Rileva le patch mancanti Microsoft® e non Microsoft®.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » Agente Windows Update
Aggiornamenti non di sicurezza mancanti	Elenca i service pack installati Microsoft® e non Microsoft®.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » Agente Windows Update

Dati	Descrizione	Porte	Protocollo
Service pack e aggiornamenti cumulativi installati	Elenca le patch installate Microsoft® e non Microsoft®.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » Agente Windows Update
Aggiornamenti di sicurezza installati	Elenca i service pack installati Microsoft® e non Microsoft®.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » Agente Windows Update
Aggiornamenti non di sicurezza installati	Elenca le patch installate Microsoft® e non Microsoft®.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » Agente Windows Update

17.2 Porte

Dati	Descrizione	Porte	Protocollo
Porte TCP aperte	Controlla la presenza di porte TCP aperte	Tutte le porte abilitate nel profilo di scansione	Socket di Windows
Porte UDP aperte	Controlla la presenza di porte UDP aperte	Tutte le porte abilitate nel profilo di scansione	Socket di Windows

17.3 Hardware

Dati	Descrizione	Porte	Protocollo
Dispositivi di rete	Elenca le schede di rete fisiche e virtuali	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.

Dati	Descrizione	Porte	Protocollo
Unità locali	Elenca le unità rilevate sulle destinazioni sottoposte a scansione. Le unità locali includono: » Dischi rigidi » Unità CD/DVD » Unità floppy	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.
Processori	Elenca i processori rilevati durante una scansione	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.
Schede madri	Elenca le schede madri rilevate durante una scansione	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.
Dettagli memoria	Restituisce informazioni di memoria relative alle destinazioni scansionate, tra cui: » Memoria fisica totale » Memoria fisica libera » Memoria virtuale totale » Memoria virtuale libera.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.
Dettagli archiviazione	Elenca ogni periferica di archiviazione rilevata durante una scansione. Le periferiche di archiviazione includono: » Dischi rigidi » Dischi rigidi virtuali » Dischi rimovibili » Unità floppy » Unità CD/DVD	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.
Schede video	Elenca le schede video rilevate durante una scansione	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.

Dati	Descrizione	Porte	Protocollo
Periferiche USB	Elenca tutte le periferiche USB rilevate collegate alle destinazioni di rete/scansione.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.
Altri dispositivi	Elenca periferiche generiche rilevate durante una scansione, tra cui: » Periferiche/driver di sistema » Human Interface Devices (HID) » Mouse e tastiera » Porte di comunicazione (seriali e parallele) » Controller disco floppy » Controller disco rigido	» TCP 139 » TCP 445 » DCOM 135 » DCOM dinamica	» SMB » Condivisione file e stampanti » Registro di sistema remoto » WMI.

17.4 Software

Dati	Descrizione	Porte	Protocollo
Applicazioni generali	Enumera ogni applicazione installata nelle destinazioni di scansione.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Applicazioni antiphishing	Elenca le applicazioni antiphishing	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Applicazioni antispyware	Elenca le applicazioni antispyware	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Applicazioni antivirus	Elenca le applicazioni antivirus.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto

Dati	Descrizione	Porte	Protocollo
Applicazioni di backup	Elenca le applicazioni di backup	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Prevenzione perdita dati	Elenca le applicazioni di prevenzione perdita di dati.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Controllo di accesso periferiche	Elenca le applicazioni di controllo di accesso periferiche.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Crittografia unità	Elenca le applicazioni di crittografia unità.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Applicazioni firewall	Elenca le applicazioni firewall	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Agente di sicurezza	Elenca le applicazioni per il monitoraggio dell'integrità del sistema.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Messenger istantaneo	Elenca le applicazioni di messaggistica istantanea.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto

Dati	Descrizione	Porte	Protocollo
Applicazioni di gestione patch	Elenca le applicazioni di gestione patch	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Peer to peer	Elenca le applicazioni peer to peer (P2P).	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Filtro URL	Elenca le applicazioni del filtro Web.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Software computer virtuale	Elenca il software di virtualizzazione rilevato in rete.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Applicazioni client VPN (Virtual Private Network)	Elenca le applicazioni client VPN	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Applicazioni browser Web	Elenca i browser web	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto

Nota

Per un elenco completo delle applicazioni di sicurezza supportate, inclusi i fornitori e i prodotti, , consultare: http://go.gfi.com/?pageid=security_app_fullreport

17.5 Informazioni di sistema

Dati	Descrizione	Porte	Protocollo
Condivisioni	Elenca tutte le condivisioni rilevate durante una scansione. Le informazioni delle condivisioni includono: » Nome condivisione » Nota di condivisione » Percorso di condivisione » Autorizzazioni di condivisione	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Criterio password	Elenca la configurazione del criterio password	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Criterio controllo di protezione	Configurazione criterio controllo di protezione	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Registro di sistema	Elenca le informazioni selezionate dal registro di sistema. Tra le informazioni enumerate: » Proprietario registro di sistema » Numero build attuale » Tipo attuale » Versione attuale » identificativo fornitore » Tipo di software	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Nomi NetBIOS	Elenca i nomi NetBIOS delle destinazioni scansionate. Questo nodo include: » Servizio workstation » Nome dominio » Servizi file server » Scelte servizio browser	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Computer	Elenca gli identificatori computer, tra cui: » Indirizzo MAC » Durata (TTL) » Ruolo di rete » Numero di serie sistema operativo » Lingua » Tipo di computer (fisico o virtuale)	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto

Dati	Descrizione	Porte	Protocollo
Gruppi	Elenca i gruppi locali o del dominio/gruppo di lavoro	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Utenti	Elenca gli utenti locali o del dominio/gruppo di lavoro	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Utenti connessi	Elenca gli utenti connessi localmente e in remoto	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Sessioni	Elenca le sessioni attive al momento della scansione.	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Servizi	Elenca ogni servizio rilevato durante una scansione	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
Processi	Elenca ogni processo attivo rilevato durante una scansione	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto
TOD (ora del giorno) in remoto)	Elenca l'orario corrente e il tempo di attività delle destinazioni scansionate	» TCP 139 » TCP 445	» SMB » Condivisione file e stampanti » Registro di sistema remoto

18 Appendice 2 - Certificazioni

GFI LanGuard è certificato OVAL e CVE. Le sezioni che seguono illustrano tutte le certificazioni e ne spiegano la modalità di utilizzo in GFI LanGuard.

Argomenti del presente capitolo:

18.1 Open Vulnerability and Assessment Language (OVAL) 268

18.2 Common Vulnerabilities and Exposures (CVE) 269

18.1 Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL™) è uno standard internazionale della comunità di sicurezza informatica per promuovere contenuto sulla sicurezza aperto e accessibile al pubblico, nonché standardizzare il trasferimento di tali informazioni attraverso l'intera gamma di strumenti e servizi di protezione. OVAL comprende un linguaggio utilizzato per codificare i dettagli di sistema e numerosi archivi di contenuto disponibili in tutta la comunità OVAL. Il linguaggio consente di standardizzare le tre fasi principali del processo di valutazione:

- Rappresentazione delle informazioni di configurazione dei sistemi per la verifica
- Analisi del sistema per verificare la presenza dello stato di un determinato computer (vulnerabilità, configurazione, stato delle patch, ecc.)
- Resoconto dei risultati di questa valutazione
- Gli archivi sono raccolte di contenuto aperto e accessibile al pubblico che utilizzano il linguaggio.

La comunità OVAL ha sviluppato tre schemi XML per definire la struttura e il vocabolario del linguaggio OVAL. Questi schemi corrispondono alle tre fasi principali del processo di valutazione:

- Uno schema delle caratteristiche del sistema OVAL per rappresentare le informazioni di sistema
- Uno schema di definizione OVAL per esprimere lo stato di un determinato computer
- Uno schema di risultati OVAL per segnalare i risultati di una valutazione

Il contenuto scritto in linguaggio OVAL si trova in uno dei tanti archivi della comunità. Uno di questi archivi, noto come l'archivio OVAL, è ospitato da MITRE Corporation. Si tratta del punto di incontro in cui la comunità OVAL può discutere, analizzare, memorizzare e divulgare le definizioni OVAL. Ogni definizione contenuta nell'archivio OVAL specifica se una determinata vulnerabilità software, problema di configurazione, programma o patch è presente in un sistema.

La comunità della sicurezza informatica contribuisce allo sviluppo di OVAL partecipando alla creazione del linguaggio OVAL sul relativo forum degli sviluppatori e scrivendo definizioni per l'archivio OVAL attraverso il forum della comunità. Il comitato OVAL, costituito da rappresentanti provenienti da una vasta gamma di settori, dal mondo universitario e da organizzazioni governative internazionali, sovrintende e approva il linguaggio OVAL controllando la pubblicazione delle definizioni ospitate sul sito Web OVAL. Ciò significa che OVAL, fondato da US-CERT presso il Dipartimento per la sicurezza interna degli Stati Uniti (Department of Homeland Security) per la comunità, riflette le idee e la competenza condivisa della più vasta rete di professionisti nel campo dell'amministrazione dei sistemi e della sicurezza a livello mondiale.

18.1.1 Supporto OVAL in GFI LanGuard

GFI LanGuard supporta tutti i controlli definiti nel file XML pubblicato da OVAL, a eccezione dei controlli HP-UX.

GFI LanGuard non supporta i computer basati su HP-UX. Per questa ragione tali controlli non sono inclusi nell'ambito del relativo database delle definizioni dei controlli.

18.1.2 Informazioni sulla compatibilità OVAL

La compatibilità OVAL è un programma volto a promuovere la coerenza all'interno della comunità di sicurezza informatica relativamente all'uso e all'implementazione di OVAL. L'obiettivo principale del programma di compatibilità consiste nel creare un insieme di orientamenti volti a promuovere un'implementazione standard. In questo modo gli utenti saranno in grado di distinguere e acquisire familiarità con i prodotti compatibili sapendo che l'implementazione di OVAL coincide con lo standard definito.

Per acquisire la compatibilità OVAL ufficiale, un prodotto o un servizio devono aderire ai **Requisiti e raccomandazioni per la compatibilità OVAL** e completare il processo di compatibilità OVAL formale.

La compatibilità OVAL significa che GFI LanGuard incorpora OVAL secondo un metodo standard predefinito e che utilizza tale linguaggio per comunicare dettagli su vulnerabilità, patch, impostazioni di configurazione della protezione e altri stati dei computer.

18.1.3 Invio di rapporti degli errori OVAL

Qualsiasi problema relativo a GFI LanGuard o all'elenco dei controlli OVAL incluso in GFI LanGuard deve essere riferito a GFI attraverso le sue linee di assistenza ufficiali.

GFI Software Ltd si impegnerà ad analizzare ogni problema riportato e, qualora riscontrasse incoerenze o errori, pubblicherà gli aggiornamenti per risolvere tali problemi. Generalmente, gli aggiornamenti relativi ai controlli delle vulnerabilità vengono pubblicati su base mensile.

18.2 Common Vulnerabilities and Exposures (CVE)

CVE (Common Vulnerabilities and Exposures, Vulnerabilità ed esposizioni comuni) è un elenco di nomi standardizzati per le vulnerabilità e altre esposizioni nella sicurezza delle informazioni. Il suo scopo consiste nella standardizzazione dei nomi per tutte le vulnerabilità ed esposizioni nella sicurezza note al pubblico.

Si tratta di un dizionario volto a facilitare la distribuzione dei dati attraverso diversi database di vulnerabilità e strumenti di protezione. CVE semplifica la ricerca di informazioni in altri database, ma di per sé, non deve essere considerato come un database delle vulnerabilità.

CVE viene mantenuto attraverso un impegno collaborativo a livello di comunità informatica noto come CVE Editorial Board (Comitato editoriale CVE). Il Comitato editoriale comprende rappresentanti di numerose organizzazioni che si occupano di sicurezza informatica tra cui fornitori di strumenti di sicurezza, istituzioni accademiche e governative ed esperti di sicurezza informatica. CVE è gestito da MITRE Corporation che funge da moderatore delle discussioni del comitato editoriale.

18.2.1 Informazioni sulla compatibilità CVE

“CVE-compatible” significa che uno strumento, un sito Web, un database o un servizio utilizza i nomi CVE per fornire riferimenti incrociati con altri archivi che utilizzano denominazioni CVE. I prodotti e servizi “CVE-compatible” devono soddisfare i quattro requisiti riportati di seguito:

Table 93: Compatibilità CVE

Compatibilità	Descrizione
Funzionalità di ricerca CVE	Un utente deve essere in grado di cercare vulnerabilità e informazioni correlate utilizzando il nome CVE.

Compatibilità	Descrizione
Risultato CVE	Le informazioni fornite devono contenere la relativa denominazione CVE.
Mappatura	Il proprietario dell'archivio deve fornire una mappatura relativa a una versione specifica del CVE e deve impegnarsi in buona fede per assicurarne l'accuratezza.
Documentazione	La documentazione standard dell'organizzazione deve includere una descrizione del CVE, la compatibilità CVE e i dettagli sul modo in cui i clienti possono utilizzare le funzionalità CVE del proprio prodotto o servizio.

Nota

Per una comprensione approfondita della compatibilità CVE, consultare l'elenco completo dei requisiti CVE disponibile all'indirizzo: http://go.gfi.com/?pageid=LAN_CVE_Requirements

18.2.2 Informazioni su CVE e CAN

I nomi CVE (detti anche "numeri CVE", "ID CVE" e "CVE") sono identificativi comuni univoci per le vulnerabilità nel campo della sicurezza informatica note al pubblico. I nomi CVE hanno lo stato "entry" o "candidate". I nomi CVE possono avere stato "Entry" (voce) o "Candidate" (candidato). Lo stato Entry indica che il nome CVE è stato accettato nell'elenco CVE mentre lo stato Candidate (detto anche "candidati", "numeri candidati" o "CAN") indica che il nome è oggetto di valutazione ai fini dell'inclusione nell'elenco.

Ogni nome CVE comprende quanto segue:

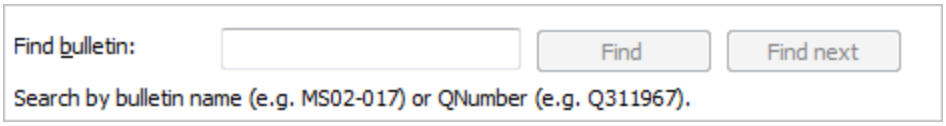
- Numero identificativo CVE (ad es. "CVE-1999-0067").
- Indicazione dello stato Entry o Candidate.
- Breve descrizione della vulnerabilità o dell'esposizione alla vulnerabilità della sicurezza.
- Eventuali riferimenti pertinenti (rapporti sulla vulnerabilità e avvisi o ID OVAL).

Nota

Per una comprensione approfondita dei nomi CVE e CAN, consultare: http://go.gfi.com/?pageid=cvecert

18.2.3 Ricerca di voci CVE

Le voci CVE possono essere cercate a partire dal nodo dei profili di scansione nella scheda Configurazione.



Screenshot 171: Ricerca di informazioni CVE

Per cercare un determinato bollettino CVE:

1. Specificare il nome del bollettino (ad esempio, CVE-2005-2126) nella casella dello strumento di ricerca nella parte inferiore del riquadro destro.

2. Fare clic su **Trova** per avviare la ricerca della voce desiderata.

18.2.4 Recupero dei nomi CVE

È possibile recuperare i nomi delle voci CVE tramite l'interfaccia utente di GFI LanGuard a partire dal nodo dei profili di scansione nella scheda Configurazione. Per impostazione predefinita, l'ID CVE viene visualizzato per tutte le vulnerabilità che dispongono di un ID CVE.

18.2.5 Importazione ed esportazione dei dati CVE

I dati CVE possono essere esportati mediante lo strumento della linea di comando Impex. For more information, refer to Utilizzo di impex.exe (page 234).

19 Glossario

A

Access™

Un sistema di gestione del database relazionale per desktop Microsoft® presente nel pacchetto Microsoft® Office. Access™ normalmente viene utilizzato per database di dimensioni ridotte.

Active Directory™ (AD)

Tecnologia che fornisce numerosi servizi di rete, inclusi servizi per directory simili a LDAP.

Agente patch

Un servizio in background che gestisce la distribuzione delle patch, dei service pack e degli aggiornamenti software nei computer di destinazione.

Antispyware

Una contromisura software che rileva lo spyware installato su un computer a insaputa dell'utente.

Antivirus

Una contromisura software che rileva il malware installato su un computer a insaputa dell'utente.

Apache web server

Un progetto server HTTP open source sviluppato e gestito da Apache software foundation.

B

Blacklist

Un elenco di nomi di periferiche USB o di rete che sono ritenute pericolose. Se durante la scansione di una rete viene rilevata una periferica USB/di rete il cui nome è nella blacklist, GFI LanGuard segnalerà la periferica come minaccia per la sicurezza (vulnerabilità a rischio di sicurezza elevato).

Bluetooth

Un protocollo di interfaccia e di comunicazione senza fili aperto che consente lo scambio di dati tra dispositivi.

C

Common Gateway Interface (CGI)

Uno script di comunicazione utilizzato dai server web per il trasferimento di dati a un browser internet client.

Common Vulnerabilities and Exposures (CVE)

Un elenco di nomi standardizzati per vulnerabilità e altre informazioni sulle falle di sicurezza. Lo scopo del CVE è di standardizzare i nomi di tutte le vulnerabilità e falle di sicurezza note

pubblicamente.

D

Dashboard

Una rappresentazione grafica dello stato delle varie operazioni che potrebbero essere attive o pianificate.

Database Microsoft® Access™

Un sistema di gestione del database relazionale per desktop Microsoft® presente nel pacchetto Microsoft® Office. Microsoft® Access™ normalmente viene utilizzato per database di dimensioni ridotte.

Demilitarized Zone (DMZ)

Un segmento di una rete che non fa parte della rete interna e che non è direttamente collegato ad Internet. Normalmente ha lo scopo di fungere da gateway tra le reti interne e Internet.

deploycmd.exe

Uno strumento riga di comando di GFI LanGuard, utilizzato per distribuire le patch di Microsoft® e software di terze parti sui computer di destinazione.

Disinstallazione automatica

Un'operazione che consente la disinstallazione automatica delle applicazioni che supportano la disinstallazione invisibile all'utente all'interno di GFI LanGuard.

DMZ

Un segmento di una rete che non fa parte della rete interna e che non è direttamente collegato ad Internet. Normalmente ha lo scopo di fungere da gateway tra le reti interne e Internet.

DNS

Un database utilizzato dalle reti TCP/IP che consente la traduzione dei nomi host in numeri IP e di fornire altre informazioni relative al dominio.

Domain Name System

Un database utilizzato dalle reti TCP/IP che consente la traduzione dei nomi host in numeri IP e di fornire altre informazioni relative al dominio.

Download automatico

Una tecnologia di GFI LanGuard che scarica automaticamente le patch e i service pack mancanti di Microsoft in tutte le 38 lingue.

E

Extensible Markup Language (XML)

Uno standard di testo aperto utilizzato per definire i formati dei dati. GFI LanGuard utilizza questo standard per importare o esportare i risultati e le configurazioni salvate.

F

File batch

Un file di testo contenente una raccolta di istruzioni che devono essere eseguite dal sistema operativo o da un'applicazione.

File Transfer Protocol

Un protocollo utilizzato per il trasferimento dei file tra i computer di rete.

FTP

Un protocollo utilizzato per il trasferimento dei file tra i computer di rete.

G

Gestione automatica delle patch

Una tecnologia di GFI LanGuard che scarica in automatico gli aggiornamenti mancanti di Microsoft® e li distribuisce nella rete.

GFI EndPointSecurity

Una soluzione di protezione sviluppata da GFI che consente alle organizzazioni di conservare l'integrità dei dati impedendo l'accesso e i trasferimenti non autorizzati dalle periferiche rimovibili.

GPO

Sistema di gestione e configurazione centralizzato di Active Directory che controlla le attività che possono eseguire gli utenti in una rete di computer.

H

Host locale

Definito come host locale nelle reti, corrisponde al computer attualmente in uso. Si può fare riferimento all'host locale utilizzando l'indirizzo IP riservato 127.0.0.1. Nel presente manuale, per host locale si intende il computer dove è installato GFI LanGuard.

I

impex.exe

Uno strumento della riga di comando, utilizzato per importare ed esportare profili e vulnerabilità da GFI LanGuard.

Info bollettino

Contiene una raccolta di informazioni relative a una patch o a un aggiornamento Microsoft®. Utilizzata all'interno di GFI LanGuard per fornire maggiori dati su un aggiornamento o patch installata. Le informazioni includono: id bollettino, titolo, descrizione, URL e dimensioni file.

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) è uno dei protocolli di base di Internet Protocol Suite. Viene utilizzato dai sistemi operativi dei computer di rete per inviare messaggi di

errore che indicano, per esempio, che un servizio richiesto non è disponibile o che un host o un router non possono essere raggiunti. ICMP può anche essere utilizzato per inoltrare i messaggi di query.

Internet Information Services (IIS)

Una serie di servizi basati su Internet creati da Microsoft® Corporation per i server di Internet.

L

LAN Wi-Fi/Wireless

Una tecnologia usata comunemente nelle reti di aree locali. Per la comunicazione, i nodi della rete utilizzano i dati trasmessi su onde radio al posto dei cavi.

Linux

Un sistema operativo open source che fa parte della famiglia del sistema operativo Unix.

lnsscmd.exe

Uno strumento della riga di comando di GFI LanGuard che consente l'esecuzione di controlli di vulnerabilità sui computer di destinazione della rete.

M

Malware

Il malware, ovvero il software dannoso, è un termine generale utilizzato per tutto il software che mira a danneggiare e colpire il sistema di un computer. Virus, worm e trojan sono tutti tipi di malware.

Microsoft® IIS

Una serie di servizi basati su Internet creati da Microsoft® Corporation per i server di Internet.

Microsoft® WSUS

Un acronimo per Microsoft® Windows Server Update Services. Questo servizio consente agli amministratori di gestire la distribuzione degli aggiornamenti Microsoft® nei computer di rete.

Modulo SSH

Un modulo utilizzato per determinare il risultato dei controlli di vulnerabilità attraverso i dati (testo) della console prodotti da uno script eseguito. Ciò significa che è possibile creare dei controlli personalizzati di vulnerabilità Linux/UNIX tramite qualsiasi metodo di scripting che è supportato dal sistema operativo Linux/UNIX del computer di destinazione e che fornisce alla console i risultati in formato testo.

N

NETBIOS

Un acronimo per Network Basic Input/output. Questo sistema fornisce servizi per consentire la comunicazione tra applicazioni su computer diversi all'interno della rete.

Netscape

Un browser web originariamente sviluppato da Netscape Communications Corporation.

O

Oggetto Criteri di gruppo (GPO)

Sistema di gestione e configurazione centralizzato di Active Directory che controlla le attività che possono eseguire gli utenti in una rete di computer.

Open Vulnerability and Assessment Language (OVAL)

Uno standard che promuove contenuto di sicurezza aperto e pubblicamente disponibile e standardizza il trasferimento di tali informazioni nell'intero spettro di strumenti e servizi di sicurezza.

OVAL

Uno standard che promuove il contenuto di sicurezza aperto e pubblicamente disponibile e standardizza il trasferimento di tali informazioni nell'intero spettro di strumenti e servizi di sicurezza.

P

Ping ICMP

Internet Control Message Protocol (ICMP) è uno dei protocolli di base di Internet Protocol Suite. Viene utilizzato dai sistemi operativi dei computer di rete per inviare messaggi di errore che indicano, per esempio, che un servizio richiesto non è disponibile o che un host o un router non possono essere raggiunti. ICMP può anche essere utilizzato per inoltrare i messaggi di query.

Porte TCP

Acronimo di Transmitting Control Protocol. Questo protocollo è stato sviluppato per consentire alle applicazioni di trasmettere e ricevere i dati su Internet attraverso le "well-known ports" del computer.

Porte UDP

Un acronimo per User Datagram Protocol, utilizzato per trasferire i dati UDP tra le periferiche. In questo protocollo non vengono riconosciuti i pacchetti ricevuti.

Profili di scansione

Una raccolta di controlli di vulnerabilità che determina quali falle identificare e quali informazioni recuperare dalle destinazioni scansionate.

Programma backdoor

Un metodo alternativo utilizzato per accedere a un computer o ai dati di un computer tramite la rete.

R

Remote Desktop Protocol

Un protocollo sviluppato da Microsoft® per consentire ai client di connettersi all'interfaccia utente di un computer remoto.

Riparazione automatica

Una tecnologia di GFI LanGuard che scarica e distribuisce automaticamente le patch mancanti. Se un'applicazione viene inserita nella blacklist di GFI LanGuard, la riparazione automatica disinstallerà l'applicazione dal computer di destinazione nel corso delle operazioni pianificate.

S

SANS

Un acronimo dell'organizzazione di ricerca System Administration, Networking and Security. Un istituto che condivide soluzioni per avvisi di sistema e di sicurezza.

Script Debugger

Un modulo di GFI LanGuard che consente di scrivere ed eseguire il debug di script personalizzati mediante un linguaggio compatibile con VBScript.

Script Python

Un linguaggio di script di programmazione per computer ad alto livello.

Server di posta

Il server che gestisce e archivia i messaggi del client.

Server Web

Un server che fornisce le pagine web ai browser client utilizzando il protocollo HTTP.

Service pack di Microsoft® Windows

Una raccolta di aggiornamenti e correzioni fornite da Microsoft® per migliorare un'applicazione o un sistema operativo.

Servizi Terminal

Un servizio che consente la connessione a un computer di destinazione e che ne gestisce le applicazioni installate e i dati archiviati.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol è una tecnologia utilizzata per il monitoraggio di periferiche di rete quali router, hub e switch.

SNMP

Acronimo di Simple Network Management Protocol, una tecnologia utilizzata per il monitoraggio di periferiche di rete quali router, hub e switch.

Spyware

Un tipo di malware finalizzato alla raccolta di informazioni da un computer a insaputa dell'utente.

SQL Server®

Sistema di gestione di database relazionali Microsoft®. Microsoft® include funzionalità extra per SQL Server® (controllo transazioni, gestione eccezioni e sicurezza) affinché Microsoft® SQL Server possa supportare organizzazioni di grandi dimensioni.

Strumenti Enumera utenti

Uno strumento che consente il recupero degli utenti e delle informazioni relative ad essi dal dominio/gruppo di lavoro.

Strumento Controllo del server SQL Server

Uno strumento utilizzato per verificare la vulnerabilità delle password dell'account 'sa' (ovvero dell'amministratore di rete) e qualsiasi account utente SQL configurato su SQL Server.

Strumento controllo SNMP

Uno strumento che segnala la presenza di stringhe comunità deboli, eseguendo un attacco a dizionario con i valori memorizzati nel dizionario predefinito.

Strumento Enumera computer

Un'utilità che identifica i domini e i gruppi di lavoro in una rete.

Strumento esplorazione SNMP

Uno strumento utilizzato per indagare i nodi di rete e recuperare le informazioni SNMP.

Strumento Ricerca DNS

Un’utilità che converte i nomi dei domini negli indirizzi IP corrispondenti e recupera informazioni specifiche dal dominio di destinazione.

Strumento Traceroute

Uno strumento utilizzato per identificare il percorso seguito da GFI LanGuard per raggiungere un computer di destinazione.

Strumento Whois

Uno strumento che consente di cercare le informazioni su un particolare dominio o indirizzo IP.

T

Trojan

Un tipo di malware contenente un'applicazione nascosta in grado di danneggiare un computer.

U

Uniform Resource Locator (URL)

Uniform Resource Locator è l'indirizzo di una pagina web nel world wide web.

Universal Serial Bus (USB)

Uno standard di bus seriale ampiamente utilizzato per connettere le periferiche a un computer host.

URL

Uniform Resource Locator è l'indirizzo di una pagina web nel world wide web.

V

VBScript

Un linguaggio di Visual Basic Scripting è un linguaggio di programmazione ad alto livello sviluppato da Microsoft®.

Virus

Un tipo di malware in grado di danneggiare un computer. Lo scopo di un virus è di danneggiare un computer corrompendone i file e le applicazioni. Un virus è un programma autoreplicante e può copiarsi in tutto il sistema di computer.

W

Whitelist

Un elenco di nomi di periferiche USB o di rete che sono ritenute pericolose. Quando il nome di una periferica di rete/USB rilevata durante la scansione della rete contiene una voce inserita nella whitelist, GFI LanGuard ignorerà la periferica, considerandola come un'origine sicura.”

X

XML

Uno standard di testo aperto utilizzato per definire i formati dei dati. GFI LanGuard utilizza questo standard per importare o esportare i risultati e le configurazioni salvate.

20 Indice

A

Agente 17, 19, 23, 41, 46, 49, 53, 55, 62, 65, 83-85, 95, 97, 104, 121, 130, 141, 143, 158, 165, 217, 260, 264

Agenti relay 17, 19, 25, 54, 95

Aggiorna 46

Aggiornamenti di sicurezza 39, 97, 123, 149, 158, 165, 205

Aggiornamenti di sicurezza installati 113, 147, 168, 261

Aggiornamenti di sicurezza mancanti 112, 144, 165, 260

Aggiornamenti non di sicurezza installati 113, 147, 261

Aggiornamenti non di sicurezza mancanti 113, 144, 260

Aggiornamenti prodotto 163

Aggiornamento automatico 190

Aggiornamento di 26

Antispyware 166

Applicazioni client VPN 115, 265

Applicazioni firewall 115, 168, 264

Applicazioni generali 115, 263

Applicazioni non autorizzate 96, 98, 166, 214

Attendant service 18

Attività 18, 24, 45-46, 65, 67, 72, 83, 85, 95, 120, 122, 127, 143-144, 156, 162-164, 173, 190, 194, 219-221, 223-224, 226-230, 267

Attributi 48, 51, 63, 88, 90, 98, 166

Avanzate 46, 52, 54-55, 89, 121, 134, 137, 139, 147, 149, 151-152, 154, 177, 184, 204, 212, 252

B

Basato su scansione - Controllo completo 166

Browser web 98

C

Centro riparazioni 92, 124, 137, 143, 149, 151, 153, 155

Certificazioni 268

CGI 205

Cliente 259

Componenti 18, 23, 31-32, 256

Computer 17, 19, 23, 30, 32, 35, 37, 39, 41, 43-44, 46, 49, 53, 55, 62, 67, 72-73, 82, 84-86, 90, 93-94, 97, 101-103, 108, 120, 123, 129-130, 135, 137, 141, 143, 146, 149-152, 154, 158, 160-161, 165, 171, 173, 179, 181, 188, 198, 211, 219, 221, 223, 225, 228-229, 231, 242, 246, 254, 265-266, 268

Condivisione file e stampanti 25, 260-261, 263, 266

Condivisioni 54, 67, 116, 132, 149, 167, 210, 219, 266

Condivisioni aperte 166

Condizioni 168, 195, 239, 243, 249, 254

Conformità 43, 164

Confronto di base 167

Connessione desktop remoto 154

Console di gestione 18

Controller disco floppy 263

Controllo 16, 18, 21, 26, 31-32, 46, 55, 63, 67-68, 71-72, 85, 95, 97, 100, 102-105, 111, 124, 144, 164, 190, 196, 208, 218, 226, 228, 230, 237, 242, 246, 252-253, 255, 260, 264

Controllo completo 166

Controllo rete e software 43, 65, 107, 118-119

Controllo SNMP 228

Controllo software 42-43, 67, 166

Criterio controllo di protezione 72, 116, 266

Cronologia di scansione 167

Cronologia riparazioni 167

Cronologia sicurezza di rete 167

CVE 269

D

Dashboard 40-41, 46, 49, 59, 71, 83-86, 90, 92-94, 100-106, 109, 233

deploycmd.exe 231

Dettagli archiviazione 115, 262

Dettagli memoria 115, 262

Dettagli ultima scansione 166

Digest giornaliero 184

Disinstalla 46

Disinstalla aggiornamenti software 143-144, 147

Disinstalla applicazioni 143-144

Dispositivi di rete 67, 111, 211, 261

Distribuisci aggiornamenti software 137, 143-144

Distribuzione automatica 17, 19, 44, 62, 78, 120-121, 160

Distribuzione software personalizzato 40, 42, 143, 149

DNS 53, 111, 220

download automatico 16, 124, 160, 190

Driver 116, 263

E

Editor dei profili di scansione 18, 194-195, 206, 218, 238, 243, 248

Elenco dei computer sottoposti a scansione 184

Enumera computer 41, 225, 256

Enumera utenti 227

Esplorazione SNMP 229

G

Gruppi 20, 45, 62, 85, 89, 91, 95, 98, 109, 167, 174, 225, 267

H

Hardware 23, 41-42, 67, 89, 93, 98, 105, 115, 166, 212, 261

Human Interface Devices (HID) 263

I

IIS 111

impex.exe 234

In tempo reale 93, 216, 225

Info bollettino 112, 145

Informazioni di sistema 41-42, 66, 93, 98, 106, 116, 169, 208, 266, 268

Installazione di 17, 19, 29, 31-32, 36, 76, 111, 230, 232

L

Livello 66, 85, 92, 94, 97, 109, 165, 212, 239, 243, 249, 268-269

lnsscmd.exe 231

M

Messaggi 120, 137, 175, 184

Microsoft Access 35

Modifiche di sicurezza ultima scansione 166

Mouse e tastiera 263

N

NetBIOS 26, 143, 218, 225, 252, 266

Non autorizzato 111, 214

Notifiche 18, 184

O

Open Vulnerability and Assessment Language 268

Operazioni di riparazione 17, 25, 79, 137, 144, 147, 149, 151-152, 154, 160, 166

Opzioni di avviso 79, 175, 183, 231

opzioni di conservazione database 190

Opzioni di scansione del dispositivo 212

Opzioni di scansione delle applicazioni 214

OVAL 198, 268, 270

P

Panoramica sicurezza computer 165

Panoramica sicurezza di rete 165

Password 34, 46, 71, 116, 150, 152-153, 184, 191, 205, 230-231, 246, 266

PCI DSS 43, 168

Personalizzato 45, 66, 134, 144, 149, 176, 232, 241, 245, 247

Pianificazione controllo 46

Porte 23, 27, 66, 93, 95, 103, 114, 166, 209, 219, 235, 256, 260-261, 263, 266

Porte aperte 98, 166

Porte TCP aperte 98, 261

Porte UDP aperte 98, 261

Processori 98, 115, 262

Profili 65, 195-196, 206, 209, 218, 232

Profili di scansione 18, 27, 65, 104, 120-121, 126, 194-195, 206, 208, 218, 231, 238, 243, 248, 270

Programmi di utilità 220, 223-225, 227-230

Proprietà personalizzate destinazione 69

Protocolli 25

Proxy 39, 159, 190, 205

Python 237, 242

R

Registro di sistema 111, 167, 219, 266

Registro di sistema remoto 25, 260-261, 263, 266

Ricerca DNS 220

Ricerca nel testo completo 180

Riepilogo computer 165

Riepilogo ultima scansione 166

Riferimenti 198, 239, 243

Riparazione automatica 27, 39, 46, 50, 63, 73, 85, 95, 120, 122, 130, 137, 141, 180

S

Scansioni complete/combinate 66, 218

Scansioni di sicurezza 18, 72, 156, 164, 168, 218

Scansioni pianificate 39, 72, 82, 95, 127, 158, 183

Schede madri 262

Schede video 115, 262

Script 144, 219, 231, 237, 242, 246

Script Debugger 237

Server 17-19, 23, 39, 52, 54, 64, 66, 68, 95, 111, 165, 175, 184, 190, 205, 219, 221, 230-231, 253-254, 266

Service pack e aggiornamenti cumulativi installati 97, 113, 147, 167, 261

Service pack e aggiornamenti cumulativi mancanti 97, 112, 144, 260

Sessioni 117, 267

SMB 26, 255, 260-261, 263, 266

SMTP 184

SNMP 26, 67, 218, 228-229

Software 16, 23, 30, 39-43, 67, 82, 93, 96, 98, 104, 111, 120-121, 132, 143-144, 147, 149, 158-159, 191, 206, 208, 226, 232, 263, 266, 269

SQL 25, 118, 184, 230, 254

SSH 25, 71, 76, 219, 246

Stato dell'applicazione di patch 97, 165

Stato dell'applicazione di patch al sistema 113, 260

Stato vulnerabilità 165

Strategia di gestione delle vulnerabilità 39

Strumenti riga di comando 18, 231

Struttura computer 49, 55, 62, 68, 83, 86, 90, 130, 145, 148-149, 161, 171, 174, 180

T

Traceroute 223

Trova 67, 122, 152-153, 205, 207, 254, 268, 270

U

Ultima riparazione automatica 166

Unità locali 115, 262

USB 66, 211, 263

Utenti 98, 111, 137, 169, 227, 229, 237, 256, 258, 267, 269

Utenti connessi 89, 117, 267

V

Valutazione del livello di vulnerabilità 107

Valutazione delle vulnerabilità 16, 27, 65, 107, 118-119, 195, 206, 237, 242

VBscript 237

Verifica hardware 67, 166

Vulnerabilità 16, 18, 34, 39-43, 65-66, 73, 92-94, 97, 101, 109, 120, 133, 143, 152, 165, 183, 190, 194-195, 207, 211, 218, 230-231, 237, 243, 246, 269

Vulnerabilità di sicurezza di livello alto 66, 111, 248

Vulnerabilità di sicurezza di livello basso 111, 169

W

Wake-on-LAN 71, 77, 120, 135

Whois 224

WINS 253

WMI 17, 25, 219, 261

STATI UNITI D'AMERICA, CANADA E AMERICA CENTRALE E DEL SUD

15300 Weston Parkway, Suite 104, Cary, NC 27513, Stati Uniti tel:

Telefono: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

REGNO UNITO E REPUBBLICA D'IRLANDA

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, Regno Unito

Telefono: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPA, MEDIORIENTE E AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telefono: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA E NUOVA ZELANDA

83 King William Road, Unley 5061, South Australia

Telefono: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®